



Table of Contents

1	Introduction	4
1.1	Mesh@work products.....	5
1.2	Indoor Models	5
1.3	Outdoor Models.....	5
1.4	Outdoor Long Distance Models.....	6
1.5	MeshControllers	6
1.6	How to read the display LEDs on Mesh@work products.....	7
2	Building Wireless Mesh Network with Mesh@work products	8
2.1	Basics of Compex wireless mesh network	8
2.2	Connecting PC (without wireless) to mesh network	9
2.3	Planning the MeshPoints installation.....	9
2.4	Select Operating Frequency Band of Mesh Network	10
2.5	Assigning IP Addresses to Wireless Clients.....	10
2.6	NAT Mode	10
2.7	Bridging Mode	11
3	CloudController and Mesh Network Configuration.....	12
3.1	Management Versions	12
3.2	CM and MC Primary Functions	12
4	Getting Started	13
4.1	Step 1: Create an account	13
4.2	Step 2: Add and Configure the MeshPoints in CloudController.....	13
5	Building Compex MeshSpan Network	22
5.1	How to setup and configure a MeshSpan network	23
5.2	Configuration Overview.....	25
5.2.1	Step 1 – Create and Configure Mesh Network A, B and C.....	25
5.2.2	Step 2 – Create a MeshSpan network	25
5.2.3	Step 3 – Add MeshPod to MeshSpan	25
5.2.4	Step 4 – Upload map	25
5.2.5	Step 5 – Configure the MeshPod	25
5.3	Executing the configuration steps from CloudController	26
6	Setup Broadband Aggregation on the Mesh Network	31
6.1	How to setup parallel broadband using multiple broadband routers.....	31
7	Setup HotSpot@work on the Mesh Network.....	33
7.1	How Hotspot@work works	33
7.2	Enabling Hotspot@work	33
7.3	Monitoring and managing user access from Hotspot management	34
7.4	Overview	35

8	Reporting	36
8.1	Performance Report.....	36
8.1.1	Users Log Per MeshPoint Report.....	36
8.1.2	Users Log vs Time Report.....	37
S1	Special Configurations	38
S1.1	Bridge Mode	38
S1.1.1	Setup VLAN Tagged over MeshPoint WAN port.....	38
S1.1.2	Multiple gateways using bridge connection to Company LAN network.....	39
S1.2	Setting up a Wireless Mesh System without Internet and MeshController.....	40
S1.3	Customizing of individual MeshPoint	42
A1	APPENDIX I	44
A1.1	Users Access Conditions.....	44
A1.2	Open.....	44
A1.3	User Agreement.....	44
A1.4	Hotspot@work.....	45
A1.5	Customized Internet Access Controller.....	45
A2	APPENDIX II	46
A2.1	Connecting to the existing network.....	46
A2.2	Scenario 1: Using WAN port to connect to company's existing network.....	46
A2.3	Scenario 2: Using LAN port to connect to company's existing network	46
A2.4	Scenario 3: Using both WAN and LAN ports to connect to existing network	47
A3	APPENDIX III	48
A3.1	How to add MeshPoints using Import File method.....	48
A3.2	How to add MeshPods using Import File method	49
M1	System tools.....	50
M1.1	Changing the MeshController IP Address	50
M1.2	Setting the NTP server on MeshController.....	50
M1.3	Instructions on Resetting the MeshController.....	51
M1.4	How to manually update a MeshController firmware.....	51
M1.5	How to manually update a MeshPoint firmware	53
M1.6	Installer Tools (Only on CloudManager).....	54
M1.6.1	Changing MP Check-In IP Address.....	54
M1.6.2	Changing MP Mesh ID	56
G1	Glossary Terms	59

1 Introduction

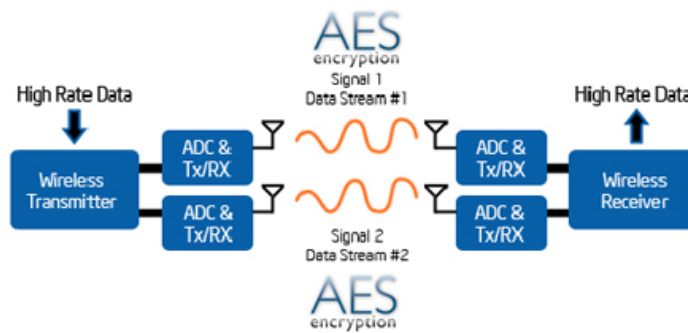
Mesh@work technology employs MeshPoints to create a wider coverage from various gateways. Highly secured backhaul links coupled with 11n technology, gives customers a seamless wireless experience. With a CloudController, customers can easily monitor their networks and quickly detect unusual activities.

Secured, High Speed Coverage

Mesh@work uses Advanced Encryption Standard (AES - 128), coupled with 802.11n technology on the backhaul, giving a high bandwidth and secured connection throughout the entire mesh network.

Secured, High Speed Backhaul

Mesh@work allows integrators to set WPA - AES on the coverage channels, coupled with 802.11n technology, giving a high bandwidth and secured connection from the users to the mesh network.



Increased Redundancy

Mesh@work (either on internet –based CloudManager or Embedded MeshController) offers increased redundancy. It ensures that MeshPoints are always check-in to a Fail-Over-Dashboard, in case the original server is not reachable.

Easy Management and Configuration

Mesh@work allows integrators to set up and customize their network, according to their local conditions. Updated released versions of firmware can be uploaded to the server, so that all the MeshPoints would be automatically updated.

Reports

Mesh@work allows various reporting modes, giving integrators a clear view of the health of the mesh network.

Hotspot

Mesh@work allows integrators to set the user access conditions: Open Access Mode, User Agreement Login Mode, Hotspot or HotZone (hereby named as Hotspot@work) or Customized Internet Access Controller, to maximize their advertising revenue.

1.1 Mesh@workK products

Compex has a full range of wireless products for building small to large wireless mesh networks. These products help you build and connect your wireless mesh network over long distance.

1.2 Indoor Models

MeshPoint MP546



Specifications	Dual radio (5GHz, 2.4GHz) 802.11n, 26dBm TxPower(aggregate) @5GHz, 20dBm TxPower (aggregate)@ 2.4GHz 2x2 2dBi omni antenna , 24VDC power adapter, 802.3af POE Compatible
Mesh type	Indoor mesh node
Application	Suitable for medium to high application access

MeshPoint MPE72



Specifications	Single radio 2.4GHz 802.11n, 26dBm TxPower (aggregate), 2x 2dBi omni antenna , 24VDC power adapter, 24V passive POE compatible
Mesh type	Indoor mesh node
Application	Suitable for low application access, internet web browsing

1.3 Outdoor Models

MeshPoint MPS546



Specifications	Dual radio (2.4GHz, 5GHz) 802.11n, 29dBm TxPower(aggregate), Built-in 6.5dBi@2.4GHz / 7dBi@5GHz dual polarized omni-directional antenna , 24VDC power adapter, 802.3af POE Compatible
Mesh type	Outdoor mesh Backhaul and Coverage MP
Application	Long distance connection, up to 300m Suitable for medium to high access applications.

MeshPoint MPS72



Specifications	Single radio (2.4GHz) 802.11n, 26dBm TxPower(aggregate), Built-in 6.5dBi dual polarized omni-directional antenna, 24VDC power adapter, 24V passive POE Compatible
Mesh type	Outdoor Coverage MP
Application	Long distance connection, up to 300m. Suitable for low application access, internet web browsing

1.4 Outdoor Long Distance Models

MeshPod MPJ72



Specifications	Single radio (5GHz) 802.11n, 29dBm TxPower(aggregate), Built-in 17dBi dual polarized directional antenna, 24VDC passive POE Compatible
Mesh type	Outdoor MeshSpan Backhaul link
Application	Long distance connection, up to 5km with good transfer speed

1.5 MeshControllers

MC100



Specifications	Managed up to 15 Mesh nodes, 100 Users Internal Flash drive storage. 24VDC power adapter
Mesh type	MeshController (Table top low profile model)
Application	CloudManager and Hotspot Manager, Broadband Aggregation.

MC200



Specifications	Managed up to 30 Mesh nodes, 100 Users Internal Hard Disk storage 110VAC/240VAC power input
Mesh type	MeshController (Rack mount, 1U type)
Application	CloudManager, Hotspot Manager, Broadband Aggregation.

1.6 How to read the display LEDs on Mesh@work products

The MeshPoints front panel display LEDs are arranged as follows: (from left to right)






Models	Ethernet	Front Panel Display LEDs
MP546, MPS546	2 ports. POE connection at WAN port.	Front panel LEDs display 
MPE72, MPS72,	2 ports. LED status is on the ports . POE connection at the LAN port.	Front panel LEDs display 
MPJ72	2 ports. POE connection at LAN port.	Front panel LEDs display 

Table 1.6a –Panel Display LEDs

The 4 LEDs color; red, orange, green and green, have different status indications for different products.

MeshPoints and MeshPods

a) When the MeshPoint is a **Mesh Gateway**,

Gateway LEDs status	Connection Status
 All 4 LEDs light up	Connected and able to check-in to CCM / MC
 All 4 LEDs no light	Not connected or check-in to CCM / MC

b) When the MeshPoint is a **Repeater** (mesh node)





Repeater LEDs status	Quality of Link with Gateway
 All 4 LEDs light up	Excellent
 3 LEDs light up	Good
 2 LEDs light up	Fair
 1 LEDs light up	Poor

Table 1.6c –Mesh node (Repeater) LEDs status

MeshController

When operating in normal mode.





LEDs status	Process Status
 Red LED blink continuously	No Internet connection
 Orange LED light up	USB Flash /Hard disk detected
 First Green LED light up	Database is up
 Last Green LED light up	Radius is up

Table 1.6d –MechController LEDs status

2 Building Wireless Mesh Network with Mesh@work products

2.1 Basics of Complex wireless mesh network

The following are the components and characteristics of Complex wireless mesh network:

- Complex wireless mesh network can be build with 3 or more mesh nodes.
- The wireless mesh network is configured and managed from the internet –based CloudManager or Embedded MeshController (a device installed on the network).
- The wireless mesh network consists of mesh nodes and mesh gateway(s).
- Complex mesh node or mesh gateway is a MeshPoint (MP) device, e.g. **MP546, MPE72 (indoor)** and **MPS546, MPS72 (outdoor)**.
- Each MeshPoint has two Ethernet ports: WAN (routing) port and LAN (bridge) port.
- The mesh gateway connects to upstream wire network with shared resources.

MeshPoint connects an Ethernet cable to one of its Ethernet ports takes on one of the two roles when connecting the wireless mesh network to the upstream wire network.

- The MeshPoint becomes a **mesh gateway** when its WAN port is connected to the existing network and obtains an IP address from an Internet router. NAT mode is enabled the MP.
- The MeshPoint becomes a **mesh bridge** when its LAN port is connected to the existing network and DHCP packets are passed transparently from the existing network to the mesh.

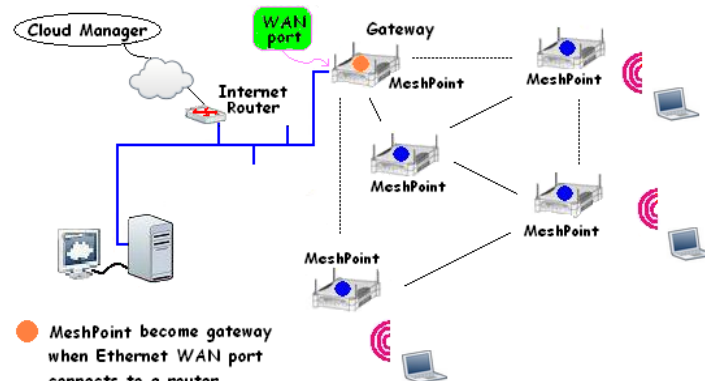


Fig 2.1a –mesh gateway

For a large wireless mesh network, multiple MeshPoints located at strategic location can become mesh gateways.

Advantages of having multiple gateways:

- They provide alternative routes that creates shorter link paths for end nodes. This helps reduce latency and increase transfer speed across the network.
- They provide multiple connections to the network shared resources which helps avoid single point failure.

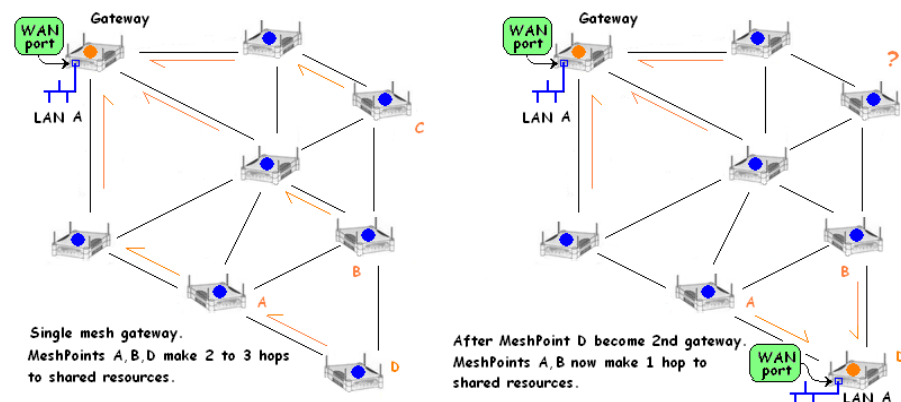


Fig 2.1b –multiple mesh gateway

2.2 Connecting PC (without wireless) to mesh network

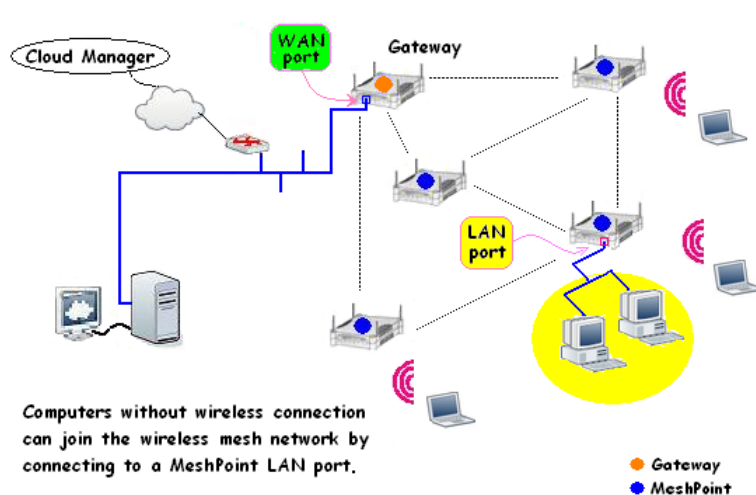


Fig 2.2a –PC joining the mesh network

PC without wireless connection can connect with Ethernet cable to a MeshPoint LAN port to join wireless mesh network. When there are several PCs, then a switch is used to connect them to the MeshPoint.

Note, that this type of connection to the MeshPoint LAN port is called a **mesh bridge**.

*** Note:**
Currently, multiple mesh bridges cannot be connected to a same switch. Network loopbacks can happen.

2.3 Planning the MeshPoints installation

Compex Mesh@workK products do not require to pre-configuration of individual devices prior to installation. The devices, which come with default settings, can be installed directly out of box. MeshPoints will be reconfigured and managed later from the CloudController.

The initial installation requires the MeshPoints to be placed at locations within range to be discovered by it neighboring MeshPoints. The recommended minimum signal strength between neighboring MeshPoints is RSSI 20. As the indoor environment can be very different for different types of deployment, there is no fixed distance for placing the devices. However, the following common environment scenarios can offer a close estimate of the distance.

For better clarification, in this section, when the focus is on the MeshPoint backhaul role, we refer to it as MP and when the focus is on coverage role, we refer to it as AP instead.

Identify areas where more APs are needed to service the users.

- Identify those areas where most users will be located. Use a ratio of 1.5 AP per user to determine the number of APs required for that area. A ratio of 2 AP per user will be better. If users are not fixed or stationed at specific areas but constantly on the move, then identify areas where users are more likely to be. These APs are expected to be placed closer to ensure all users have good range and signal quality.
- Depending on the application deployment requirements, an average of 30 users per AP will be a good estimate.

Populate MP around these strategically located APs that are close to users.

- Populate MP around these strategically located APs to expand the mesh coverage area. Preferably, MPs should be positioned within LOS (line of sight) with the others. These MPs can be placed further apart but should be kept to the recommend minimum signal strength of at least RSSI 20, taking into considerations the obstacles like walls, pillars.
- All MPs should be mounted as high as possible so they can better blanket the coverage area better. Mounting too low can reduce AP's coverage which can be blocked by people, furniture, low partitions, etc.

- A Mesh network connects users to shared resources. Its possible traffic may hop over many MPs if the mesh network is large or the MPs are not placed correctly. For example, one hop reduces speed by half, two hops to a quarter, three hops to one eighth, and four hops to one sixteenth.

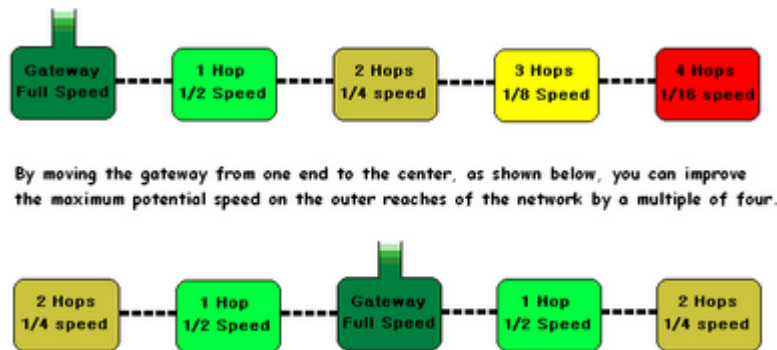


Fig 2h –Too many hops lower performance

If the MPs are not placed correctly, simply moving them closer and/or add additional MPs will correct this problem as the mesh network automatically discover new neighbors to create shorter paths.

For a large mesh network, the correct approach is to create more mesh gateways at strategic locations to break up long routes into shorter paths through these mesh gateways.

2.4 Select Operating Frequency Band of Mesh Network

Wireless interference can affect performance of a wireless network. It's important to do site survey to check for interferences such as other devices running on the same frequency or interference from overlapping of adjacent channels, noise level. Running tools like NetStumbler and NetSurvey let you view all active channels running at the site. Carefully selecting channel free of such conflicts and interferences ensures network performance.

2.4GHz frequency band has 3 non-overlapping channels while 5GHz frequency band has 23 non-overlapping channels. Most, if not all, users use 2.4GHz band. So 5GHz is the better frequency band for Backhaul operation in mesh network. Thus, Compex Dual Radio MeshPoint comes with 5GHz band radio for Backhaul operation and 2.4GHz band for Coverage operation.

In terms of wireless connection, connecting to a wireless mesh network is no different from connecting to single AP wireless network. With wireless mesh network, each MP Coverage operation presents as a connection point for the users. Thus there are more APs to choose from to connect on a wireless mesh network. Although a wireless mesh network has many APs available, users generally see only one SSID. Multiple SSIDs deployment offers multiple security connections to the different access security levels on the network.

2.5 Assigning IP Addresses to Wireless Clients

The administrator can assigned IP addresses to the wireless clients via one of the following two addressing modes. How the addressing mode is configured depends on whether the MeshPoint acts as a mesh gateway or as a mesh bridge when connected to the upstream wire network. When connected as mesh gateway, NAT mode is enabled. When connected as mesh bridge, bridging is established.

2.6 NAT Mode

In NAT mode, the Compex MeshPoint act as mesh gateway and runs as DHCP server. The IP address pool is generated automatically by the MeshPoint gateway and assigned to the wireless clients.

This is the **default mode**.

NAT mode should be enabled when any of the following is true:

- ☐ Wireless clients associated with the SSID require Internet-only access.

- ☐ There is no DHCP server on the LAN that can assign IP addresses to the wireless clients.
- ☐ There is a DHCP server on the LAN, but it does not have enough IP addresses to assign to wireless clients.

The implications of enabling NAT mode are as follows:

- ☐ Devices outside of the wireless network cannot initiate a connection with a wireless client.
- ☐ Wireless clients cannot use Layer 2 discovery protocols to find other devices on either the wired or wireless network.
- ☐ Legacy VPN clients (i.e., those that do not support NAT Traversal) may not be able to establish IPSec tunnels over the wireless network. (One workaround is to upgrade the VPN client or configure the VPN client to establish an IPSec tunnel over TCP, e.g. SSL.)
- ☐ VLAN tagging wireless traffic is not supported in NAT mode.

2.7 Bridging Mode

In bridging mode, the Compex MeshPoint acts as a mesh bridge, allowing wireless clients to obtain their IP addresses from an upstream DHCP server.

Bridge mode should be enabled when any of the following is true:

- ☐ Wired and wireless clients in the network need to reach each other (e.g., a wireless laptop needs to discover the IP address of a network printer, or wired desktop needs to connect to a wireless surveillance camera).
- ☐ Layer 2 multicast and broadcast packets (e.g., ARP, Bonjour) need to propagate in a limited manner to both wired and wireless clients for device discovery, networking, etc.
- ☐ The wireless mesh network needs to support legacy VPN clients (i.e., those that do not support NAT Traversal).
- ☐ Wired and wireless clients need to have IP addresses in the same subnet for monitoring and/or access control reasons (e.g., a web gateway in the network allows/denies Internet access based on the client's IP address).
- ☐ Wireless traffic needs to be VLAN-tagged between the MeshPoint Ethernet connection and the upstream wired infrastructure.

The implications of enabling bridge mode are as follows:

- ☐ Multiple DHCP servers are allowed, but they must assign IP addresses to wireless clients from the same subnet. This enables these IP addresses to be routed by the LAN to which the MeshPoints are connected.

3 CloudController and Mesh Network Configuration

CloudController (CC) will be used throughout the document to represent both Complex CloudManager (CM) and MeshController (MC).

This document is written based on Complex CloudManager v6.17 and MeshController v6.18.

3.1 Management Versions

There are two management versions:

□ **Complex CloudManager (CM) :**

The Complex CloudManager is an application on the Internet for customer deployment of standard wireless mesh networks that have Internet access. This Internet management application is free to companies and organizations that build their wireless network using Complex Mesh@work products to save cost on installing separate management software.

□ **Complex MeshController (MC) :**

The Complex MeshController is an embedded device with built-in hard disk and has the same Complex CloudManager application. It is installed at the network site. Information reported by the wireless network is collected and stored in the device hard disk. The device gives companies and organizations the privacy and security in managing the network and information at their own premises. The device also supports additional functions: Hotspot (Hotspot@work) and Broadband Aggregation.

MC Models

MC100, MC200 : Enables companies to setup secure wireless LANs, with Hotspot capabilities. Examples include offices, warehouses and retail stores.

MC300 : Enables larger companies to setup secure wireless LANs, with Hotspot capabilities to about 1000 end users. Examples include educational campuses, and healthcare institutions.

3.2 CM and MC Primary Functions

Primary functions:

An administrator uses the CM and MC to configure and monitor Complex wireless mesh networks. The CM and MC provide the following primary functions:

□ **Centralized configuration:**

- Access to configuration settings via a web browser
- Fail-over-CloudManager ensures continuous accessibility

□ **Centralized Control, monitoring and reporting:**

- Four control methods to manage users' connection on the network
- Upload/Download Bandwidth control
- Report System with usage statistics, login history, and alerts

Additional MC functions:

□ **Hotspot@work**

- Setup and managing hotspot for offices and hotspot sites with a billing system

□ **Broadband Aggregation**

- Aggregate up to 4 Internet routers for sharing and connection load balancing on the network

4 Getting Started

This chapter describes how to configure a Compex wireless mesh network for the first time. There are 3 simple steps in creating and configuring a Compex wireless network:

Step 1: Create an account.

To manage Compex wireless mesh networks through the CC, an administrator needs to first register as a user to create a login account.

The administrator then logs in with the registered user name and password to access the CC.

Step 2: Add and Configure the MeshPoints in CloudController.

After login into an account, the administrator needs to create the first wireless mesh network.

The steps include naming the network, adding MPs, and configuring the MPs with access policies.

Step 3: Test the network.

The administrator can start testing the basic settings in the wireless mesh network after the MeshPoint devices are installed.

4.1 Step 1: Create an account

Run the web browser,

- If you are using the CC, type the URL, <http://www.meshatwork.com/dashboard2>
- If you are using the MC, enter the MC's IP address, <http://192.168.0.2/dashboard>

Every network has its own IP subnet. You should enter your MC's IP address instead.

To change the MC IP address, please refer to **System Tools** chapter of this manual for [M1.1 - Changing the MeshController IP Address](#). After changing the IP address then connect using this new IP address.

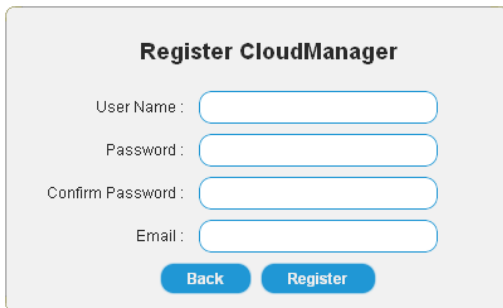
A registration form titled "Register CloudManager". It contains four input fields: "User Name", "Password", "Confirm Password", and "Email". Below the fields are two buttons: "Back" and "Register".

Fig 4.1a –CloudManager Registration Prompt

A login form titled "Sign into CloudManager v6.18". It contains two input fields: "User Name" and "Password". Below the fields are three buttons: "Forget Password", "Register", and "Login". There is also a link "Installer Tools" at the bottom right.

Fig 4.1b –CloudManager Logon Prompt

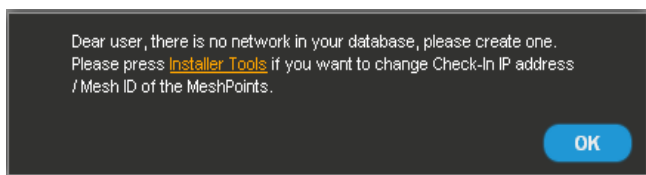
4.2 Step 2: Add and Configure the MeshPoints in CloudController

New user logging in for the first time will receive the prompt below to create the first network profile.

See fig 4.2a below. Click the **OK** button to continue.

After the first network is created, the prompt will not display on subsequent logins.

*** Note:** Ignore the message about the **Installer Tools** at the moment.
This will be covered in later chapters

A dark-themed dialog box with white text. The text reads: "Dear user, there is no network in your database, please create one. Please press [Installer Tools](#) if you want to change Check-In IP address / Mesh ID of the MeshPoints." There is an "OK" button at the bottom right.

The tools are for the following purposes:

- Change MP Check-In IP address
- Change MP Mesh ID

Fig 4.2a –First time login network prompt

a) Create a new network

First create a new network name. This will be the network profile of your first wireless mesh network.

The screenshot shows the 'Create Network' form with the following fields and options:

- Network Name:** Text input field.
- Network Email:** Text input field with 'default@dashboard.com'.
- Time Zone:** Dropdown menu with '08:00' selected.
- Location:** Dropdown menu with 'Singapore' selected.
- Scenario:** Dropdown menu with 'With Internet' selected. Annotations: 'With Internet' (Network is connected to Internet), 'No Internet' (Network not connected to Internet).
- Map Type:** Dropdown menu with 'World Map' selected. Annotations: 'World Map' (Display Google map), 'Custom Map' (Upload own map).
- Environment:** Dropdown menu with 'Outdoor' selected. Annotations: 'Outdoor' (For Backhaul link more than 150m), 'Indoor' (For Backhaul link less than 150m).
- Models in Network:** Dropdown menu with 'MP546A / MP543A / MPJ7' selected. Annotations: 'MP546A / MP543A / MPJ72' (For Dual Radio MeshPoint and MeshPod models), 'MP546G / MPE72' (For Single Radio MeshPoint models).
- Nums of SSIDs:** Dropdown menu with '2' selected.
- Create Network:** Blue button at the bottom.

Fig 4.2b –Create a new network

- Network Name** : Enter your first network profile name.
Choose a relevant name that identifies your network. When there are more networks added later it will help identify the right network promptly.
- Network Email** : Enter a valid email address. All CC notifications will be sent to this address.
- Time Zone** : Select the time zone where the network is installed.
- Location** : Select the country where the network is installed.
- Scenario** : Select **With Internet** if the network is connected to Internet.
Otherwise, select **No Internet**.
- Map Type** : When **World Map** is selected, Google Map will be the overlay map for the MPs. If you plan to upload your own map such as an office floor plan, then select **Custom Map** instead.
- Environment** : Wireless devices installed over long distance require longer respond time, such as CTS and ACK handshake during communications to ensure optimum network performance.
Options are: **Outdoor** and **Indoor**.
Select **Outdoor** when the MPs backhaul links are over 200m.
Select **Indoor** when the MPs backhaul links are less than 150m.
- Models In Network** : This selection choose the type of MP model (Single or Dual Radio type) deployed in wireless mesh network.
Select **MP543G / MPE72**, for the Single Radio MeshPoint models.
Select **MP546A / MP543A / MPJ72** for Dual Radio MeshPoint models.
- Nums of SSIDs** : By default two SSIDs will be created.
If more than two SSIDs profiles are required, then select from the box the closes number required. Available choices are: 2, 4 and 8

b) Adding MeshPoints in the new network

First add all MPs in the network.

From the menu, select the **Mesh Management tab** from the menu, click on the **Add MeshPoint button**.

Refer to the fig 4.2d (green box) below.

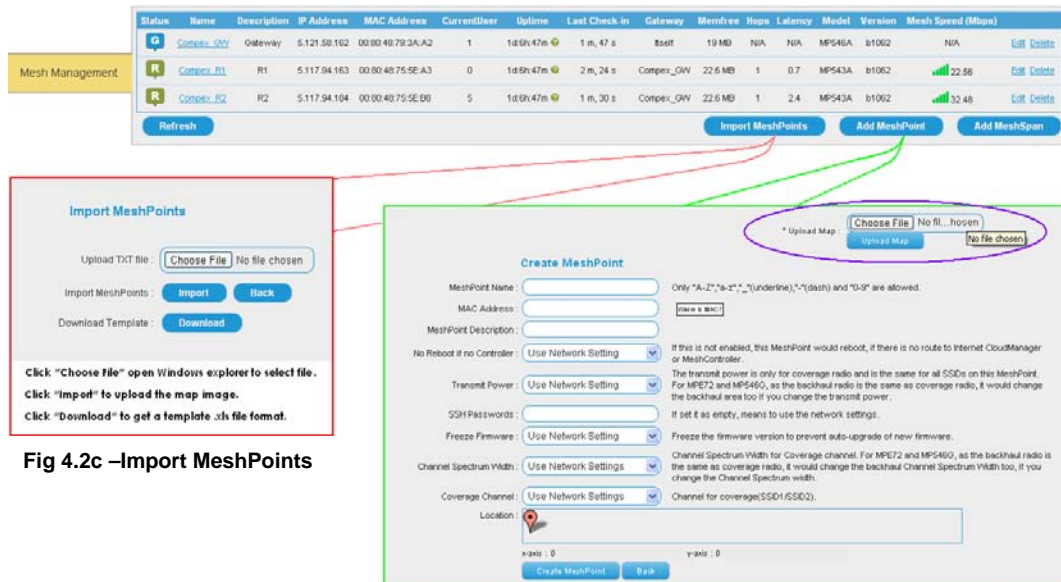


Fig 4.2c –Import MeshPoints

Fig 4.2d –Add MeshPoints

Follow the instructions below to complete the entries:


- MeshPoint Name** : Enter a short name for this MP.
- MAC Address** : Enter the **Backhaul Wireless MAC address** of this MP. Info is located at the back of each MP.

Record all MeshPoints wireless MAC addresses before installing them on site.
A recommended practice is to record all the MPs and their locations before installation.
Refer to table 4.2a below

MP546A	Wireless Backhaul MAC address	Location
MeshPoint A	00:80:48:01:01:01	At Sales dept
MeshPoint B	00:80:48:01:02:02	At Reception
MeshPoint C	00:80:48:01:03:03	At Admin dept

Table 4.2a –Recording form for MPs

MeshPoint Description : Enter info about this MP. Location will be a good reference.

Location : If World Map is selected when creating the network, Google Map will be displayed in this box. You can drag the marker  over the map to show this MP location. The Latitude and Longitude show the global positioning of the MP.
if Custom Map is selected and no map is uploaded, the box will display the marker only. To upload the map, use the Upload Map option at the top of the page. Click the **Choose File** button to browse and select the map file from your PC hard drive. Then click the **Upload Map** button to start the file upload. Drag the marker over the map to place the MP. The X-axis and Y-axis show the MP position on the map.

The others settings from the page listed below are for customizing the individual MP.
At this stage, leave these settings in their default. They will be globally configured to all the MPs in the **Advanced Settings** section of the **Network Settings** tab page later.

Globally configurable settings:

-  **No Reboot if no Controller**
-  **Transmit Power**
-  **SSH Password**
-  **Freeze Firmware**
-  **Channel Spectrum Width**
-  **Coverage Channel**

After completing, click the **Create MeshPoint** button below page to create the MP.
Repeat this step for the next MP until all the MPs are created.

If there are many MPs to add, you can use the **Import MeshPoints** button (see the **red box** in **fig 4.2c** above) to upload the Import file.
For details on how to create the import file, refer to **Appendix III, A3.1-- Add MeshPoints using the Import File method**

All MPs created are listed in the table below the map. To delete an MP that is created wrongly, e.g. wrong MAC address, click the **Delete** button for that MP to delete it. Then recreate the MP again.
If you need to change the MP name and location or upload your map, use the **Edit** button on right side.
You can only upload your own map if you have selected **Custom Map** when creating the new network.
To upload your map, click the **Choose File** button at the top of the **Edit MeshPoint** page to locate your map file in your PC hard drive. Then click the **Upload Map** button to start the file upload. After map display, drag the marker over the map to place the MP. The X-axis and Y-axis show the MP position on the map.

Recommended map file size and resolutions:

Viewing the map on iPad or any other handheld devices, select size map 900*450 pixels (1024*768 / iPad). For bigger view screen, choose a map size of 1200*450(1366*768 / 13" screen) or 1850*768(1920*1080 / 23" screen).

See **fig 4.2e** below for an example that uses office floor plan.

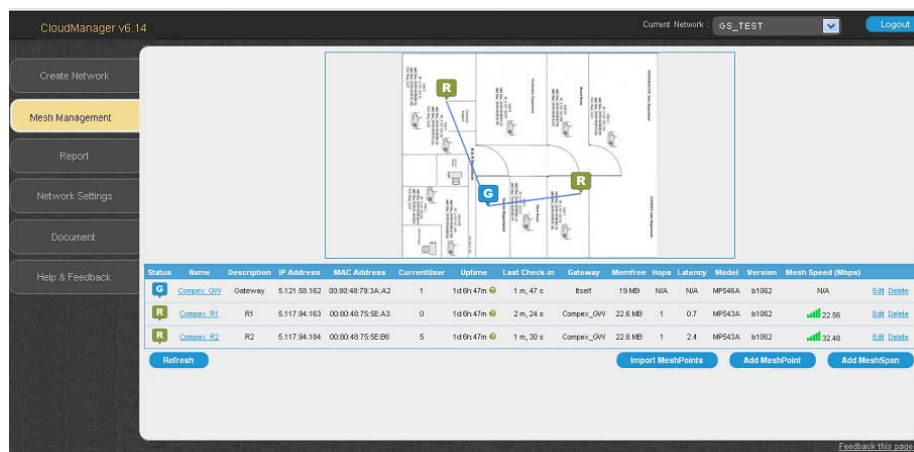


Fig 4.2e –MeshPoints table and map locations

c) Configure the MeshPoints

All these settings are done, under the **Network Settings** tab page.

This includes:

- i) Backhaul and Coverage channel setup.
Action: changing the operation channel
- ii) Configure user wireless connection profiles and Advanced Settings.
Action: o- Edit the MP connection profiles
o- Block direct user-to-user communication connected on the same MP (optional)
o- Updating the MP firmware
- iii) User Access Conditions selection.
This setup is optional. Default is Open, which means the user can freely connect on the network.
Action: Select a user access control method on the network.
- iv) Select the MPs boot recovery action (to reboot or not to) when the controller connection is lost.

To execute the steps, click the **Network Settings** tab and follow the instructions.

i) Backhaul and Coverage Channel setup For Dual Radio MeshPoints

Dual Radio MeshPoints, including **MP546A** and **MPS546A**, have one radio operating at 5GHz band for the backhaul operation and another radio operating at 2.4GHz band for the coverage operation. First set a channel for these radios. Choose channel that has no interference or conflict.

In the **Network Settings** tab page, look for the **Advanced Settings** section. See **Fig 4.2f** below.

Fig 4.2f –Configuring Dual Radio Backhaul and Coverage channels

Do the following:

- For **Country**, click to select the country the network is installed to ensure selected operation frequency will be in compliant with the requirements by the authority.
- For **Mesh Channel**, click the down arrow to select new backhaul operation channel.
- For **Coverage Channel**, click the down arrow to select new coverage channel.
If **Auto channel** is selected, the device can determine and automatically select the channel that has the least interference.

* **Note** : **Auto channel** selection is not available for Single Radio MeshPoint.

For Single Radio MeshPoints

Single Radio MeshPoints, including **MP546G** and **MPS546G/MPE72** and **MPS72**, run the backhaul and coverage operation on the same radio. Thus, under the **Network Settings** tab for **Advanced Setting** section, only the **Mesh Channel** setting with 2.4GHz band range is displayed. Selecting the **Mesh Channel** also automatically sets the same channel for coverage operation.

For this initial configuration to get the mesh network up you can ignore the reset of the settings.

Do **NOT** click the **Save Settings** button yet. Do it after completing the settings for other sections on the page.

ii) Configure wireless connection profiles and Advanced Settings

o- Edit SSID connection profiles

Backhaul security is automatically created and set up to Advanced Encryption Standard (128-bit AES) creating a highly secured connection. No further action necessary.

SSID profile is setup for the connection between the user and the MeshPoint.

By defaults, 2 profiles are created. **SSID 1 (Public)** and **SSID 2 (Private)**

Public profile default SSID name is *Meshwork* and no wireless security is enabled.

Private profile default SSID name is *mySecure* and wireless security WPA-AES-CCMP is enabled with the default WPA key, Op3nm35h

*** Note:** When creating a new network and more than two SSIDs are selected then additional SSID profiles will be displayed on the Network Settings page.

To change SSID 1 (Public) profile settings, from **Network Settings** page, look at the, **SSID 1 (Public) Settings** section.

To change SSID 2 (Private) profile settings, from **Network Settings** page, look at the **SSID 2 (Private) Settings** section.

Fig 4.2g –Configure SSID1

Fig 4.2h –Configure SSID2

Both the SSID1 (Public) and the SSID2 (Private) profiles have similar setup options and choices.

- Enable SSID 1** : Enabled by default. To disable, remove tick in the box.
- Hide ESSID** : When checked, MP will not broadcast the SSID. But user can still connect to MP with the correct SSID.
- Network Name (SSID 1 SSID)** : Enter new SSID name for this profile.
- Network WPA Key** : Leave blank if wireless connection security is not required. When box is filled with 8 characters or more, wireless security is automatically enabled. Fewer than 8 characters error will prompt an error to display.
- Use MeshPoint Name** : Default is disabled and box is not checked. When enabled or checked, each MeshPoint overwrites the SSID name set in **Network Name (SSID1 SSID)** with its default MP name as the SSID. This option is used in special applications where each MP must have a different SSID.
- Minimum Signal Strength** : This setting can affect user roaming response. 3 selectable options are, Disabled, Recommended, Aggressive.
 - Disabled** = User link may not switch over to a stronger signal MP.
 - Recommended** = User link will switch over to above average signal MP.
 - Aggressive** = User link will switch over quickly to higher signal MP.
- WPA Enterprise Server** : To connect to a WPA Enterprise 802.1x server. Enter the IP address of the server. Leave blank when not using the service.
- WPA Enterprise Port** : Enter the port number used by WPA Enterprise 802.1x server. Leave blank when not using the service.

o- Block direct user-to-user communication on the same MeshPoint

When 2 or more users are connected to an MP, they can establish direct communication with each other. Such communication may load the network unnecessarily and can be blocked.

Under Advanced Settings section there are **SSID 1 Isolation** and **SSID 2 Isolation** settings. SSID 1 applies to the SSID 1 profile and SSID 2 applies to the SSID 2 profiles. Adding a tick in the box (shown by the red arrow →) enables blockage of such direct communication among the users connected on the MP with the respective SSID connection.

Fig 4.2i –Configuring the Advanced Setting

o- Uploading the MeshPoint firmware with Compex CloudController

Newer firmware for the MP,,when available, can be automatically scheduled to upload to the MPs within an hour with minimum down time to the network.

To setup refer to the above **fig 4.2i** indicated by the blue arrow →

Open **Network Settings** tab page from the menu, on the **Advanced Settings** section, do the following:

- ✓ Remove the tick from **Freeze Firmware** box.
- ✓ Next, enter in the **Firmware Server** box, the path where the firmware file can be found.

Generally, the firmware image file is saved in your computer. So enter the path to your computer storage device shared folder. For example, computer shared folder name is **MP-Firmware** and your computer IP address is **101.58.162.43** then the path to enter will be [\\101.58.162.43/MP-Firmware](http://101.58.162.43/MP-Firmware)

The firmware update process will start within one 1 hour after activation. So ensures to keep this computer running for the next 2 hours.

- * **Note:** When update firmware become available, Compex will upload the file to the CC. If you plan to let all your MPs automatically update to newer the firmware uploaded by Compex on the CC, you can set in the **Firmware Server** box to the path, 116.12.130.110/dashboard/firmware/
Also ensures the tick in the **Freeze Firmware** box is removed.

o- Uploading the MeshPoint firmware with the MeshControler

If you are using the MC instead, the firmware file is first copied to the controller instead.

To copy the firmware to the MC, refer to above **fig 4.2j** below indicated by the blue arrow →

First open the **Network Settings** tab page from the menu, in the **Advanced Settings** section, do the following:

- ✓ Remove the tick from **Freeze Firmware** box.
- ✓ Next, enter in the **Firmware Server** box, the path where the firmware file can be found.
Recommended to use the MC default path name, my.dashboard/dashboard/firmware/

Next copy the firmware image file to the MC.

Open the **System tab page** from the menu, for the **MeshPoint Firmware Upgrade** setting, click the **Choose File** button to browse your computer hard drive locate and select the firmware file. Then click the **Upload** button to start copy the file to the MC.

In about an hour, the MPs will download the firmware image file from the MC and do the firmware upgrade.

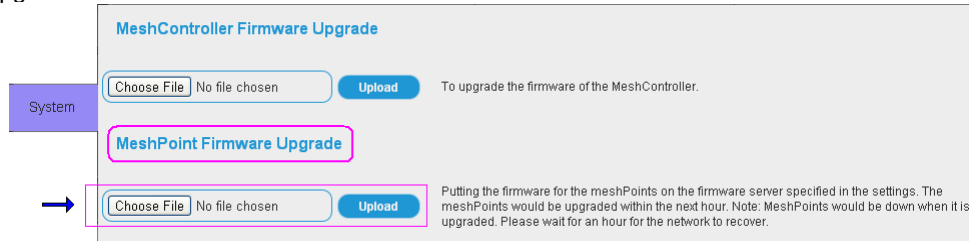


Fig 4.2j –Upload MP firmware file in MeshController

iii) User Access Conditions selection

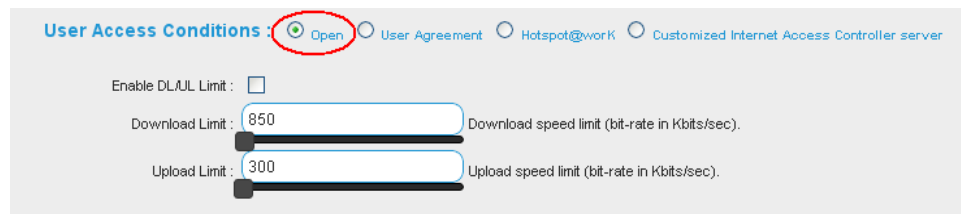


Fig 4.2k –Selecting Open option in User Access Condition

Administrator can choose a holistic control method to manage user access on the network.

There are 4 options: **Open**, **User Agreement**, **Hotspot** and **Internet Access Controller**

Select by clicking on the respective option radio button to activate it.

For configuration example, leave it as **Open**, the default setting.

If you plan to enable the download and upload speed control for all users, click on **Enable DL/UL Limit** box and add a tick. A tick in the box indicates function is enabled. Then enter the maximum speed allowed, in kilobits/sec, in the respective download and upload box.

For instructions on setup of other options, please refer **Appendix 1** section in this document.

iv) Select the MPs boot recovery action when the controller connection is lost.

By default the MPs check-in to the controller every 5 minutes in normal operation. If an MP has lost the connection with the controller it automatically reboots to recover. The recovery process may create a network connection disruption. The lost connection may just a temporary Internet connection lost. To skip the reboot action, tick on the **No Reboot if no Controller** box.




Default is not tick.

Configuration on the **Network Settings tab page** is now completed.

Click the **Save Settings** button to save and activate the configuration.

It will take about 5-10min for all MPs to reboot and reconfigured the wireless mesh network.

During the reboot, the MPs become inactive and the **Mesh Management tab page** will display the status

of the MPs with this icon, . After the MPs are up again their icon status will change; mesh nodes are indicated with the icon,  and gateways indicated with the icon, . This indicates the network is ready.

On completing these 2 steps, your mesh network is now configured and activated.

Keeping accurate date and time

If you are using the MC to manage the network, it is important for the MPs and the MC to keep accurate date and time. To setup the NTP server on the MC please refer to the System Tools chapter on [M1.2 - Setting the NTP server on MeshController](#).

4.3 Step 3 Test the network

For a new installation, the next step is to check the link signal strength or RSSI of the neighboring MPs. **Recommended: at least RSSI 20** between neighboring MPs. A higher value means MPs will develop a stronger link, thus, creating a more stable wireless mesh network and achieving higher transfer speed. To view the RSSI reading, select Mesh Management tab from the menu on the left side of page.

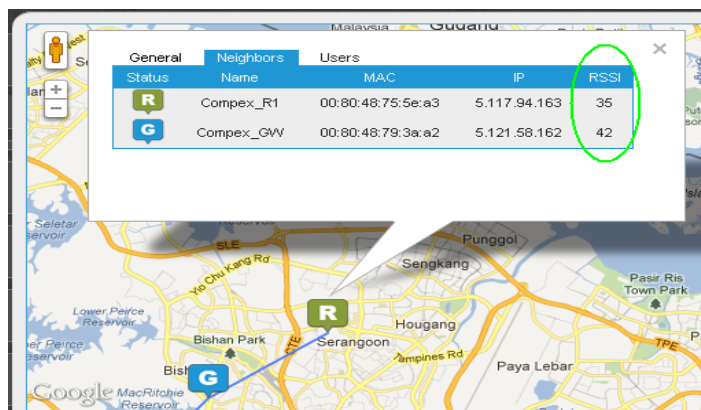


Fig 4.3a –Viewing neighbor MPs RSSI readings

Adjust the position of these MPs until all neighbor nodes attain a reading of at least RSSI 20 and higher.

To test the wireless mesh network, select a MP on the wireless mesh network as mesh gateway by connecting its WAN port to a LAN router on upstream wire network. Then connect a user to the wireless mesh network. Now proceed to check the network speed and performance with the connection.

For Internet speed check, try to connect to a website providing speed test utility. Choose a test site closest to network location. Sites far away can be quite slow and inconsistent in terms of speed and response time. Conduct local access tests by connecting to the server and run a network test. Such tests will give you an idea of the initial performance of the network.

4.4 Finalizing the Network Settings and Checkup.

After satisfied with the network operation, you can now proceed to do the following:

- ✓ Tighten security on the network
 - Activate SSID security
 - Change all MPs and MC (if use) devices default password
 - Change the Administrator password
 - ✓ Setup and check network monitoring is operating properly
 - Checking notifications sent from management can be received
 - Setup and check Fail-over-CloudManager works.
 - ✓ Fine tune the network operations
 - Setup automatic firmware update
 - Customized individual MP
 - ▶ Select non-overlapping coverage channel for nearby MP
 - ▶ Adjust the MPs coverage Transmit Power to create a more balanced signal level throughout network coverage areas.
- Disadvantages of unbalanced coverage signal strength among the MPs are:
- MP that appears with stronger signal than its neighbor MPs to their neighbor clients gets more neighbor user connections. This creates an unbalanced user connection distribution on the mesh network.
 - Affects user roaming to MP with less user connections.

For setup details, refer to the **Special Configuration chapter**, [S1.3 --Customizing individual MeshPoint](#).

Also refer to **CloudManager/MeshController User's Guide** for details explanation on the operation of these functions and setup.

5 Building Complex MeshSpan Network

Terms

Mesh Point (MP)	Complex indoor AP with mesh capabilities
Mesh node	Generic term for an AP in a mesh network
Mesh network	Generic term for a wireless mesh network built with AP connected in a mesh
MeshSpan	Complex long-distance mesh backhaul network, consisting of interconnected MeshPods
MeshPod (MPod)	Individual long-distance wireless connection devices that form a Complex MeshSpan
MeshSpan node	Consist of several MeshPods connected together through Ethernet

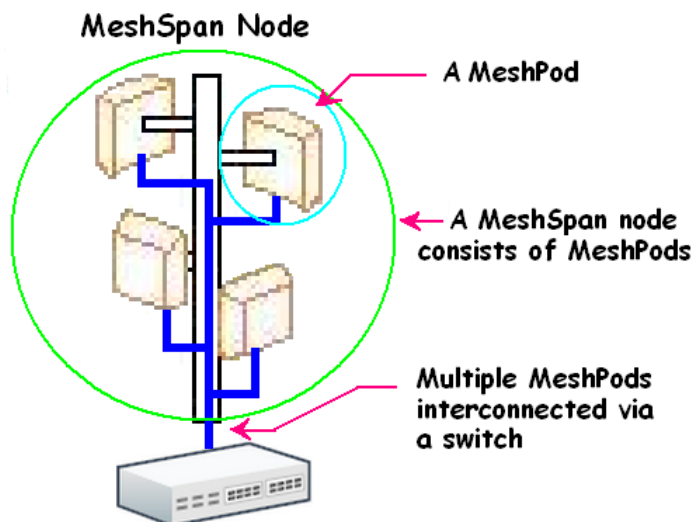


Fig 5a –MeshSpan node

MeshSpan is Complex long-distance mesh algorithm. MeshSpan nodes, located several kilometers apart, link up to form a mesh backhaul network. Each MeshSpan node consists of several Complex MeshPods (MPJ72) interconnected through Ethernet switches, mounted on the pole and installed on high-rise buildings and towers.

Figure below illustrates how MeshSpan is deployed to link multiple cluster networks at different locations to form one giant mesh network.

Advantage 1: Link up to 5km

Each MeshSpan node can link up to 5km with the transfer speed between the nodes ranging from 200Mbps to 50 Mbps, depending on the distance spanned and environmental conditions. An intermediate MeshSpan node can be installed in between, if more than 5km away. Several such MeshSpan nodes can be installed stretching the distance. Signal is received and repeated by different MeshPods of the MeshSpan node, thus the transfer speed is maintained traveling over each MeshSpan node.

Advantage 2: Common Shared Resources

Resources at distant cluster network locations can become common shared resources, or resources at one location can now be decentralized, thereby avoiding single-point connection failure that causes all resources to become unavailable. For example, an active server can be in one location while a mirror server in another. When the active server goes down or loses connection, the mirror server kicks in. Users continue to be able to access to the server without noticing the connection to the active server has been lost.

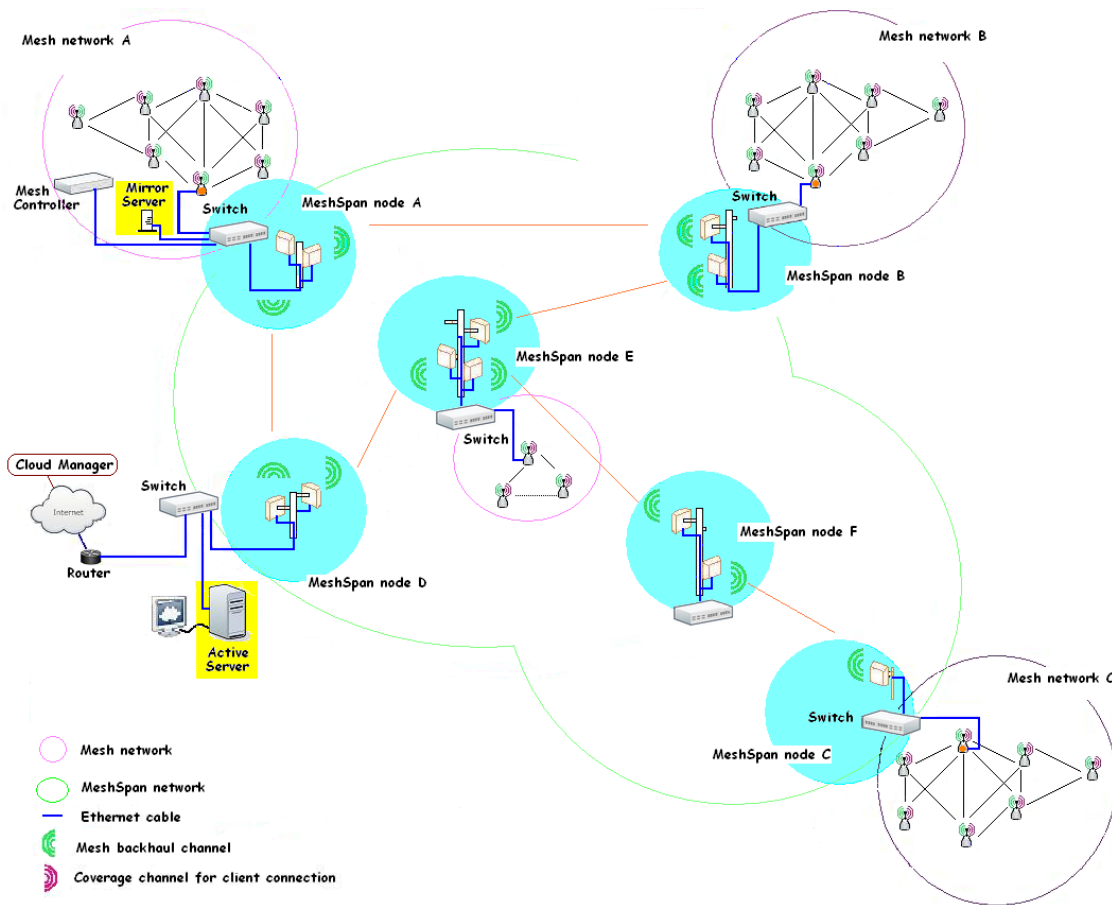


Fig 5b –An example of a MeshSpan network

The figure above shows how a hotspot service can be extended to all mesh networks using MeshSpan. With the deployment of MeshSpan, new mesh networks can easily join the MeshSpan network simply by adding a MeshSpan node.

Below is an example of how to setup and configure a MeshSpan network.

5.1 How to setup and configure a MeshSpan network

MeshSpan (**MSpan**) connects networks over a long distance. Just as a wireless mesh network is built with mesh nodes, MeshSpan is built with MeshSpan nodes. It may consist of one or more MeshPod (**MPod**) devices depending on the number of MeshSpan node (**MSnode**) links.

The example below shows how MeshSpan can be deployed to link three wireless mesh networks A, B and C into a larger wireless mesh network. Complex MeshPod **MPJ72** device is deployed. In this example, the MeshSpan node has 2pcs MeshPod devices installed at each mesh network location A, B and C. As MeshSpan node link between mesh network A and C is too far, an intermediate MeshSpan node is deployed in between. This MeshSpan node also has 2pcs MeshPod devices.

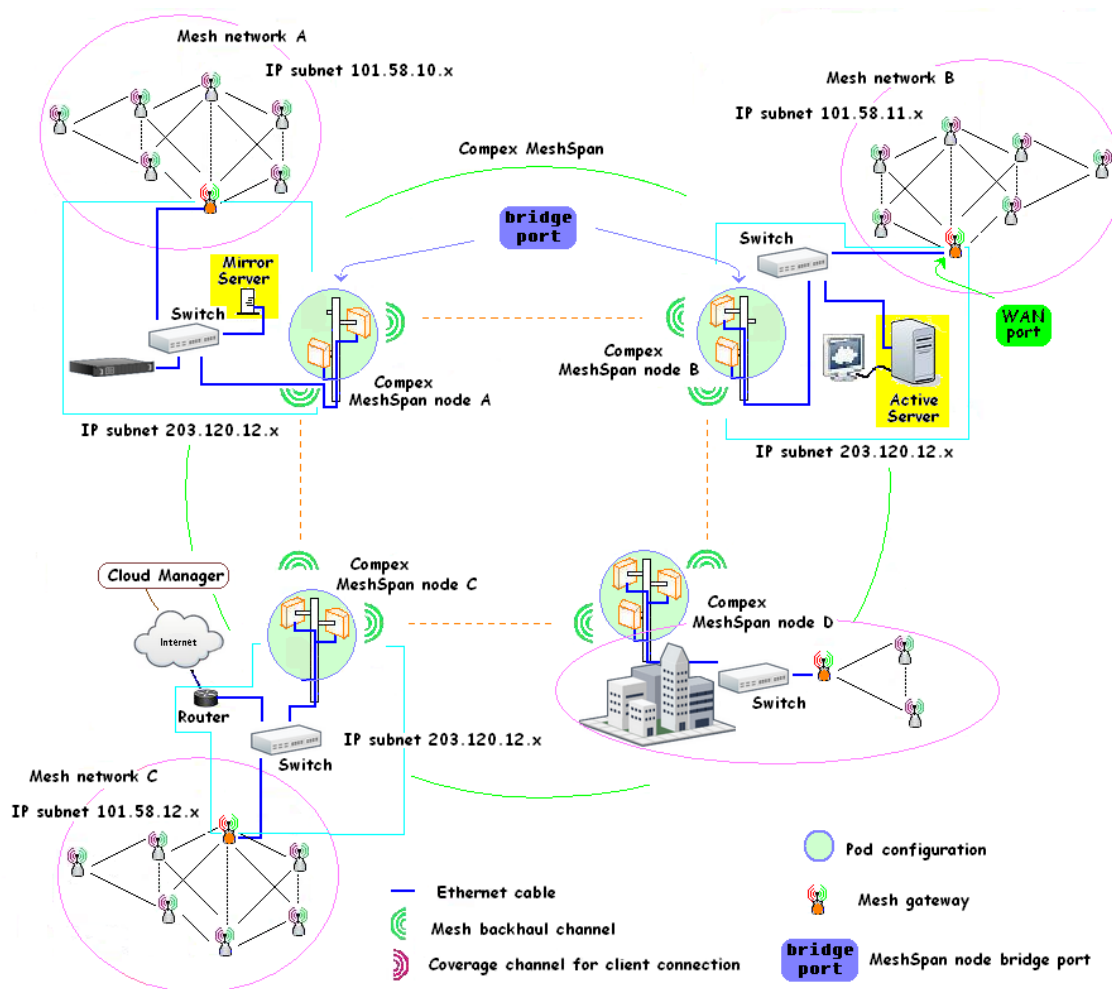


Fig 5.1a –A typical MeshSpan network

This is how they are connected:

Wireless connections

- MeshSpan node A and MeshSpan node B use one MPod device to link with each other.
- MeshSpan node A uses the 2nd MPod device to link to an MPod device of MeshSpan node C.
- MeshSpan node D uses each MPod device to link to MeshSpan node B and C 2nd MPod device.

Ethernet connections

- The 2 MPods on MeshSpan node A, B and C connect Ethernet LAN ports to the LAN switch network A, B and C respectively.
- The 2 MPods on MeshSpan node D connect the Ethernet LAN port back to back with each other.
If more than 2 MPods are mounted, then a switch is used to connect them.

Configuration is based on this example of network setup.

Each network is created and configured as a separate network from the CC. Thus the configuration is divided into 4 parts. Part 1 to 3 covers the information and configuration of mesh network A, B and C. Part 4 covers the information and configuration of MeshSpan network.

5.2 Configuration Overview

5.2.1 Step 1 – Create and Configure Mesh Network A, B and C

Part 1 to 3

If these are new mesh networks, then each must be created and configured with the CC first.

Each mesh network is to be created as a separate network.

When creating the network name, choose a name that is easy to identify e.g., Mesh-A for network A, Mesh-B for network B, and Mesh-C for network C.

5.2.2 Step 2 – Create a MeshSpan network

Part 4

Next create the MeshSpan network.

Create a new network name for this MeshSpan network, e.g., MSpan-ABC

We shall name the MeshSpan nodes at the respective mesh network site A, B and C as MeshSpan node A, MeshSpan node B and MeshSpan node C and the intermediate node as MeshSpan node D.

5.2.3 Step 3 – Add MeshPod to MeshSpan

Next, add MeshPods (**MPod**) to the MeshSpan nodes (**MSnode**).

MPods in each MSnode, if not configured, may create wireless link among themselves, preventing the node from operating properly. From the CC, first create the MSnode name, then add the MPods to the MSnode name. Adding the MPod requires entering the Wireless Backhaul MAC addresses. In this setup example there are 2 MPods on a MSnode assembly and the MPod deployed is the **MPJ72** device. The MAC address of the **MPJ72** is printed on the device label. Before installing the MSnode assembly, record each pair of the **MPJ72** Wireless Backhaul MAC addresses on each MSnode and their installation locations as shown in table below.

MPJ72	Node-A	Node-B	Node-C	Node-D
Wireless Backhaul MAC address	00:80:48:01:01:01	00:80:48:01:20:11	00:80:48:01:30:21	00:80:48:01:40:31
	00:80:48:01:01:14	00:80:48:01:20:14	00:80:48:01:30:24	00:80:48:01:40:34
Location	Building A	Building B	Building C	Building D

Table 5.2.3a –MeshSpan node MeshPod Table

For **MSnode A**

- Create a new MSnode name and label it as **Node-A**, for example.
- Add the 2 MPods devices Wireless Backhaul MAC addresses in **Node-A**

For **MSnode B**

- Create a new MSnode name and label it as **Node-B**.
- Add the 2 MPods devices Wireless Backhaul MAC addresses in **Node-B**

For **MSnode C**

- Create a new MSnode name and label it as **Node-C**.
- Add the 2 MPods devices Wireless Backhaul MAC addresses in **Node-C**

For **MSnode D**

- Create a new MSnode name and label it as **Node-D**.
- Add the 2 MPods devices Wireless Backhaul MAC addresses in **Node-D**

5.2.4 Step 4 – Upload map

This option allows you to upload your own display map. The MPods can then be placed on the map with the display of the install locations.

5.2.5 Step 5 – Configure the MeshPod

Next,

- Set the **Mesh Channel** (the wireless backhaul channel).
- Update it to the latest firmware, if available.

5.3 Executing the configuration steps from CloudController

Step 1

First create and configure the wireless mesh networks A, B and C from the CC.

They are separate networks on different locations, so each network is to be created as a separate network profile name.

When creating the network name, choose a name that is easy to identify, e.g. Mesh-A for network A, Mesh-B for network B, and Mesh-C for network C.

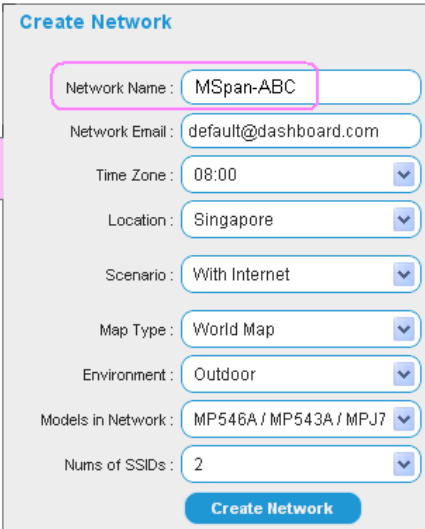
Wireless mesh network build with MPs has been covered in the earlier section.

For detailed steps, please refer to chapter 4, [Getting Started](#)

Step 2

After created the three mesh networks, A,B and C, proceed to create yet another new network profile name for the MSpan in the same CC. In this MSpan network profile you add the MSnodes and MPods.

From the CC, (refer to figure below for the following instructions)



First enter a new network name in **Create Network** page, e.g. **MSpan-ABC**

Next, type a valid email address in **Network Email** to receive notification issued from the management.

Default **Map Type** is **World Map**.

Google map will be displayed.

If you plan you display your own map then change selection to **Custom Map**.

MSpan connects over long distance. **Environment** must select **Outdoor**

Models in Network should select the list with the MPod model. Select **MP546A / MP543A / MPJ72**

Fig 5.3a –Creating a MeshSpan network

Step 3

b) Next, create the MSnode name,

From the menu, select the **Mesh Management** tab → Click on the **Add MeshSpan** button.

For **MSnode A**, label it as **Node-A**, for example.

Next, add the 2 MPod devices to **Node-A**.

To add, click the **Add MeshPod** button and enter the Wireless Backhaul MAC address of the first MPods **MPJ72**. See fig 5.3d.

Repeat to add the second MPod.

Do the same for MSnode B, C and C using label show below.

For **MSnode B**, label it as **Node-B**

For **MSnode C**, label it as **Node-C** and


For **MSnode D**, label it as **Node-D**

- **Important: Ensure MPod's MAC address entered for MSnode-A match the Wireless Backhaul MAC addresses of the two MPJ72 devices mounted on MSnode A pole. The same applies for the other MPods for MSnode B,C, and D. Create a table (Table 5.2.3a) shown above will help avoid entering the wrong MAC addresses.**

Alternatively, if there are many MPods to be added, a simpler way to create an import file and upload the file using the **Import MeshPods** button.

For details on how to create the import file, please refer to the **Appendix III** section of this document.

Mesh Management



Status	Name	Description	IP Address	MAC Address	CurrentUser	Uptime	Last Check-in	Gateway	Memfree	Hops	Latency	Model	Version	Mesh Speed (Mbps)
There is no MeshPoints in this network, please add 1 or import some of them.														

Refresh
Import MeshPoints
Add MeshPoint
Add MeshSpan

Add "MeshPod" into 'MSpan-B' MeshSpan.

Name	MAC Address	Description	Coverage
There is no MeshPoint in this MeshPod			

"MeshPod" Name :

MAC Address :

Description :

No Reboot if no Controller : Use Network Setting

Transmit Power : Use Network Setting

SSH Passwords :

Freeze Firmware : Use Network Setting

Channel Spectrum Width : Use Network Settings

Coverage Channel : Use Network Settings


Note : Please do not put the Gateway and the Repeater on the same

Add
Back

Create MeshSpan

MeshSpan Name :





MeshSpan Description :

Location : 

x-axis : 100 y-axis : 100

Add MeshPod
Add Coverage
Back

Mesh Management

Status	Name	Description	IP Address	MAC Address	CurrentUser	Uptime	Last Check-in	Gateway	Memfree	Hops	Latency	Model	Version	Mesh Speed (Mbps)
	GW	GW	5.117.142.102	00:80:48:75:8E:66	0	0d:23h:14m	4 m, 6 s	Itself	25.5 MB	N/A	N/A	MPJ72R	b1065	N/A
	Span1	span1												
	Node1	Repeater	5.117.142.87	00:80:48:75:8E:57	N/A	0d:23h:12m	1 m, 12 s	GW	28.4 MB	1	1.3	MPJ72R	b1065	16.72
	Node2	Repeater	5.117.142.84	00:80:48:75:8E:54	N/A	0d:23h:18m	2 m, 2 s	GW	28.5 MB	2	1.1	MPJ72R	b1065	18.40

Refresh
Import MeshPoints
Add MeshPoint
Add MeshSpan

Fig 5.3b –Creating MeshSpan and Adding MeshPod

In the example, the diagram shows MSnode D has an MP installed to provide coverage for the area. If your network does not plan to have coverage in the MSpan network, you can ignore this step.

To add coverage to MSnode D, click the Edit button for **Node-D**. Refer to fig 5.3b and 5.3c and add the following:

- Coverage Name** : Enter a name for this coverage MP
- MAC Address** : Enter the MAC address of this coverage MP
- Description** : Type a description for this MP device.

Click **Add button** to add this MPcoverage device.

Add "Coverage" into 'MSpan-B' MeshSpan.

Name	MAC Address	Description	Coverage
There is no MeshPoint in this MeshPod			

"Coverage" Name :

MAC Address :

Description :

No Reboot if no Controller : Use Network Setting

Transmit Power : Use Network Setting

SSH Passwords :

Freeze Firmware : Use Network Setting

Channel Spectrum Width : Use Network Settings

Coverage Channel : Use Network Settings





Note : Please do not put the Gateway and the Repeater on the same

Add
Back

Fig 5.3c –Add coverage for MeshSpan

The settings shown below are for customizing the individual MPod. At this stage, skip these settings. They will be configured through the global settings for all the MPs in the **Advanced Settings** section of the **Network Settings** tab page later.

Globally configurable settings:

- | | |
|---|---|
|  No Reboot if no Controller |  Freeze Firmware |
|  Transmit Power |  Channel Spectrum Width |
|  SSH Password |  Coverage Channel |

Step 4

The MSnode can be better viewed and represented by overlaying them on the map to show their locations. When a new network is created World Map is the default and Google Map is displayed.

If you plan to use your own map, first change **Map Type** to **Custom Map**.

Then obtain a map of the location where the MSnodes are installed. Size it down to the resolution that would quickly load and while still giving a clear view to be displayed on the management page.

Use the following guide for recommended size and resolution: 900*450 pixels (1024*768 / iPad) or 1200*450(1336*768 / 13" screen) or 1850*768(1920*1080 / 23" screen).



Fig 5.3d –Upload Map

In the **Mesh Management** tab page, click the **Add MeshPod** button. On the page, as displayed above, click the **Choose File** button and enter the filename. Then click the **Upload Map** button on the right to start the file upload. After this the map is displayed.

To position the MSnodes on the map, click the **Edit** button of each MPod in the device list table and drag the MSnode to their respective position on the map. See Fig 5.3e below.



Fig 5.3e –MeshPods location on the map

The MSnode markers on the map have no information. Information about the node is in the MPod devices. To view the device information, click the MPod name in the MPod list table below the map.

Step 5

a) Set MPod Wireless Backhaul Channel

MPod device runs backhaul operation only; thus, it is required to set the **Mesh Channel** only. Open the **Mesh Management** tab page, in the **Advanced Settings** section, click the down-arrow in the **Mesh Channel** box, select a channel number for this backhaul operation. Refer to fig 5.3f below indicated by the red arrow →

In this example, MSnode-D has a coverage MP installed. Thus, you also need to select a **Coverage Channel** for this MP.

The screenshot shows the 'Advanced Settings' page for a mesh network. The 'Network Settings' tab is selected. The 'Mesh Channel' dropdown is highlighted with a red box and a red arrow. The 'Fail-Over CloudManager' text box is highlighted with a green box and a green arrow. The 'Freeze Firmware' checkbox is checked. The 'Firmware Server' text box contains the path 'my.dashboard/dashboard/firm'. The 'Fail-Over CloudManager' text box contains the IP address '116.12.130.110/dashboard'. The 'Save Settings' and 'Delete Network' buttons are at the bottom right.

Fig 5.3f –Advanced Settings changes

b) Upload new firmware to MPod

i) Using CloudManager

To setup refer to the above fig 5.3f indicated by the blue arrow →

Open **Network Settings** tab page from the menu, on the **Advanced Settings** section, do the following:


- ✓ Remove the tick from **Freeze Firmware** box.
- ✓ Next, enter in the **Firmware Server** box, the path where the firmware file can be found.

Generally, the firmware image file is saved in your computer. So enter the path to your computer's shared folder. For example, computer's shared folder name is **MP-Firmware** and your computer IP address is **101.58.162.43** then the path to enter will be <\\101.58.162.43\MP-Firmware>. The firmware update process will start within one 1 hour after activation. So ensures to keep this computer running for the next 2 hours.

- * **Note:** When update firmware become available, Compex will upload the file to the CM. If you plan to let all your MPs automatically update to newer the firmware, you set the path name in the **Firmware Server** box to,
116.12.130.110/dashboard/firmware/
Also ensures the tick in the **Freeze Firmware** box is removed..

ii) Using MeshController

If you are using the MC instead, the firmware file is first copied to the controller.

Refer to above **fig 5.3f** above indicated by the blue arrow 

First open the **Network Settings tab page** from the menu, in the **Advanced Settings section**, do the following:

- ✓ Remove the tick from **Freeze Firmware box**.
- ✓ Next, enter the path name in **Firmware Server box** where the firmware image file can be found.
Recommended to use the MC default path name, my.dashboard/dashboard/firmware/

To copy the firmware image file to the MC, do the following:

Open the **System tab page** from the menu, select **MeshPoint Firmware Upgrade** and click the **Choose File button** to browse your computer hard drive to select the firmware image file. Then click the **Upload button** to start copy the file to the MC.

When the MPod checks there is a newer firmware in the Firmware Server path, it automatically downloads it from the MC and update.

After completing the Network Settings tab page, remembers to click **Save Settings** button to save the configurations and activate the network.

c) Setup a Fail-Over-Dashboard

This setting is optional. You can do after you are satisfied with the network tests.

Fail-over-CloudManager lets you setup a secondary CloudController. Should the current CloudController is unreachable. The MPods will switch connection to this secondary CloudController.

- * **Note:** Please **ENSURE** that your **fail-over CloudManager** server has **EXACTLY** the same settings as the original server, or else unexpected issues might arise.

To setup, select the **Network Settings tab**, look for the **Advanced Settings section** right below the page.

Refer to **Fig 5.3f** above indicated by the green arrow 

Enter the address of the secondary CloudController.

6 Setup Broadband Aggregation on the Mesh Network

Only the **MeshController** supports the **Broadband Aggregation** function.

Multiple gateway nodes (on their WAN ports) can be connected to a switch, together with shared resources. Normally, only single router can connect to the network. With Compex parallel broadband (aggregation) technology, multiple routers can be connected to provide Internet service to the multiple gateway nodes, providing more redundancy links and balancing load sharing by user connections.

6.1 How to setup parallel broadband using multiple broadband routers

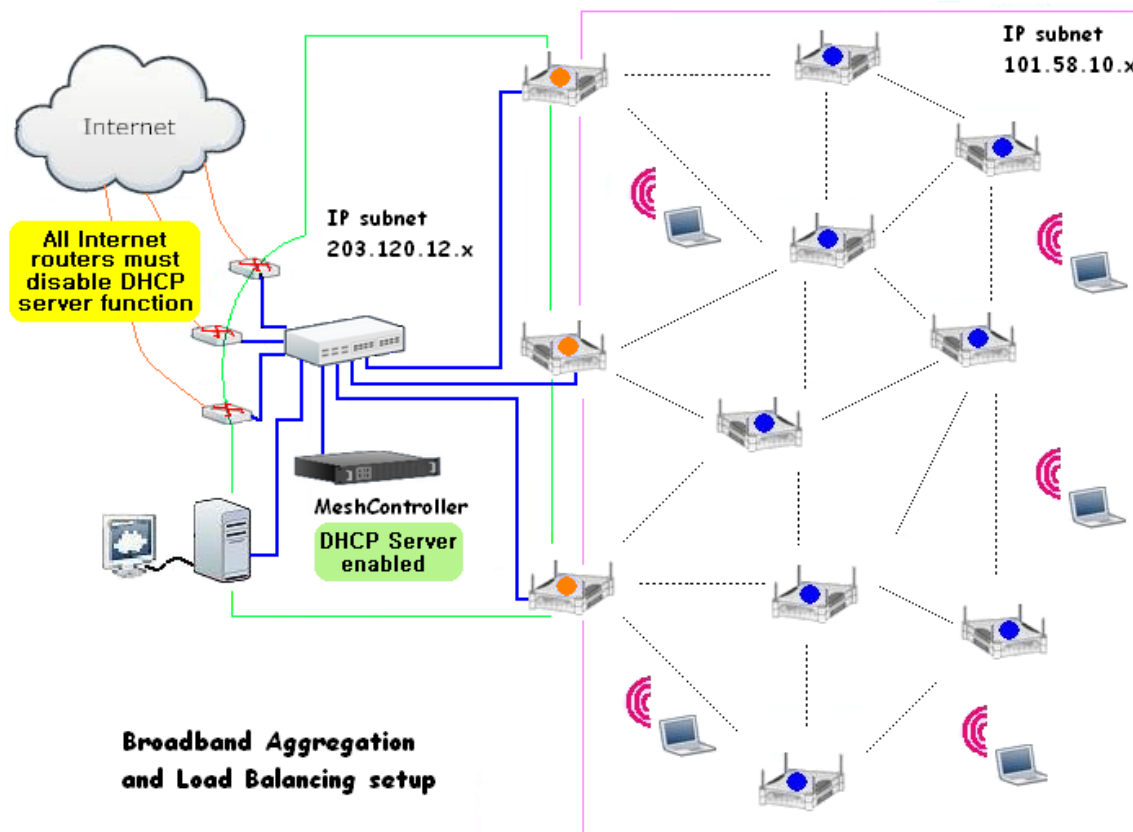


Fig 6.1a –Parallel Broadband setup

The MC can support up to four routers and any number of mesh gateways. The mesh gateways can be on one mesh network or on multiple mesh networks. The setup and configuration steps are the same.

Step 1

Disable DHCP server on all Internet routers.
Connect them to a LAN switch

Step 2

Connect MC to same LAN switch.
Run web browser and connect to MC, <http://192.168.0.2/dashboard> and login.

- **Note:** Your network might use a different IP subnet.
Use the IP address you set for your MC instead.

Select the **Bandwidth Aggregation** tab from the menu and do the following:

- a) Enable Bandwidth Aggregation by adding a tick in the box.
- b) Proceed to configure as follows:

Settings

Enable Bandwidth Aggregation : ☒

DHCP IP Range : 192.168.1.100 to 192.168.1.200

Subnet Mask : 255.255.255.0

URL/IP to check for health of the routers : http://

URL/IP List : www.google.com, www.baidu.com

This is a list of URL/IP that the MeshController would connect to check for the health of the individual routers. A "http://" would be appended to the input.

Enable Router : <input type="button" value="Enable"/>	Enable Router : <input type="button" value="Enable"/>	Enable Router : <input type="button" value="Enable"/>	Enable Router : <input type="button" value="Enable"/>
Router Name : router 1	Router Name : router 2	Router Name : router 3	Router Name : router 4
DHCP Gateway IP : 192.168.1.1	DHCP Gateway IP : 192.168.1.2	DHCP Gateway IP : 192.168.83.1	DHCP Gateway IP : 192.168.83.2
DNS IP : 61.177.7.1	DNS IP : 61.177.7.1	DNS IP : 61.177.7.1	DNS IP : 61.177.7.1

Fig 6.1b –Bandwidth Aggregation setup

Enable Bandwidth Aggregation : Check the box to enable the function.

DHCP IP Range : This is the range of IP addresses that will be assigned to clients. Enter the start IP address range in first box and the end IP range in second box.

Subnet Mask : Default is 255.255.255.0
Enter a new subnet mask to change.

URL/IP to check for health of the routers : The domain addresses are for controller to check if any of the routers has failed then it will be removed from the routers pool. Thus, domains entries must be reliable and have consistent fast response time. Enter at least two domain names.

By default all 4 routers pool entry boxes are enabled. If there are fewer than 4 routers, then disable these not in use.

For the first router pool entry:

Enable Router : Default is enabled. To disable, click the down-arrow and select Disable.

Router Name : Enter an appropriate name for the router for easy identification.

DHCP Gateway IP : Enter the IP address of the 1st router.

DNS IP : The best DNS IP address to use is the DNS IP issued by ISP to the router.
DNS IP addresses issued by ISP have the fastest response time.
Pick the first assigned DNS IP address from the router.
Enter this DNS IP address in the box.

Do the same for the other 2 routers in the pool.

Step 3

Connect all three WAN ports of the mesh gateway to the same LAN switch.

Setup is completed.

7 Setup HotSpot@work on the Mesh Network

Hotspot@work is only supported with the **MeshController**.

Complex wireless mesh network with Internet connection can easily be turned into a wireless hotspot with a billing system.

7.1 How Hotspot@work works

- 1) User buys voucher from hotspot operator before accessing the Internet.
- 2) User connects to mesh network with Internet connection.
- 3) User then runs web browser and try browse to the Internet.
- 4) User access is redirected to a captive portal that checks if user is authenticated.
- 5) If user has not been authenticated, the captive portal will then redirect the user to the login page.
- 6) User must enter the username and password issued by the hotspot operator for authentication.
- 7) User's Username/Password is authenticated by a radius server on hosted on MC database.
- 8) After the user has entered the login info (username/password), the captive portal will create an authentication request to radius server.
- 9) Radius server then checks if the request is valid by reviewing the login information stored in MySQL Database. If the information is correct, the radius server will continue to the next step, otherwise radius server will simply "reject" the request.
- 10) Next step is to check whether this account is still valid. Again if it has expired then the radius server will send a reject status to the captive portal.
- 11) If it is valid, the radius server will check the "attributes" for this account, such as connection speed, valid time, bandwidth limit, idle time out etc! If everything is fine, radius server then returns a valid status and its attributes" to the captive portal.
- 12) After sending the access acceptance status, radius server will record the usage to the database.
- 13) Captive portal then allows user to connect to the Internet with all the authentication attributes from the Radius server.
- 14) The Captive Portal will remember the attributes for the user. For instance, if one of the attributes is time limit, the captive portal will remember the time limit for the user to access the Internet.
- 15) Once user has accessed the Internet according to the given time limit, the Captive Portal will automatically disconnect the user. Then when user tries to browse the internet again the Captive Portal will request a Username and Password again before allowing user to access the Internet.

Complex hotspot has two billing systems, prepaid and postpaid.

- Prepaid system -- requires user pay first to buy voucher before accessing the hotspot.
- Postpaid system -- allows user to get the voucher first to access hotspot and pay afterwards.

With a touch of the button operator can print the voucher from the hotspot management page.

7.2 Enabling Hotspot@work

This section illustrates how to configure Hotspot@work from MC.

Hotspot@work is first enabled in MC to create hotspot managers and cashiers.

Step 1

First enable the **Hotspot@work** option in **User Access Connections** section.

Log in to the MC.

From the **Network Settings** tab page, select the radio button for **HotSpot@work** in the **User Access Conditions** section. Then click **Save Settings** button at bottom of page.

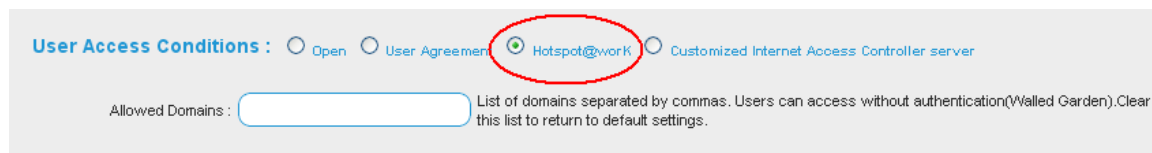


Fig 7.2a –Select Hotspot@work in User Access Conditions

Now select the **Hotspot@work** tab from the menu to create the Administrator and Cashier login accounts to manage hotspot management.

The screenshot shows the 'Hotspot@work' interface. On the left, a green tab labeled 'Hotspot@work' is selected. The main area contains a table of users and a 'Create Hotspot User' form on the right.

Name	Email	Type			
admin	pt_myat@compex.com.s	admin	Click to Login		
tham	kw_tham@compex.com.s	admin	Click to Login		
thamcashier	kw_tham@compex.com.s	cashier	Click to Login		

The 'Create Hotspot User' form on the right includes fields for Name, Password, Confirm Password, Email, and Type (set to Admin). A 'Create Hotspot User' button is at the bottom.

Fig 7.2b –Creating hotspot managers

Step 2

Create at least one administrator user and any number of cashiers.
 Administrator has the ability to add plans into the **Hotspot@work** interface, monitor the lists of users using the plans and generate vouchers for users.
 Cashier can only monitor the lists of users using the plans and generate vouchers.

To access the hotspot management page, open the web browser, type the address below and login using the account name and password.

From the web browser, connect to the MC, type the following URL:

http:// 192.168.0.2/dashboard/hotspot

*** Note:** The IP address, 192.168.0.2 is a factory default address.
 You should replace the IP address with your setup address.

The screenshot shows the 'Sign into Hotspot' login prompt. It includes a language selector (English | 简体中文), fields for User Name and Password, a 'Login' button, and a 'Back to Dashboard' link.

Fig 7.2c –Hotspot logon prompt

7.3 Monitoring and managing user access from Hotspot management

The screenshot shows the 'Hotspot@work v6.07' interface. The top navigation bar includes tabs for Prepaid, Postpaid, Office, Guest, Report, Document, and Feedback. The 'Prepaid' tab is selected, and the 'Prepaid Plan' sub-tab is active. The main area displays a table with columns: Code, Prepaid Plan, Time Used, Time Remain, Packet Used, Packet Remain, Printed / Not Printed, Usage Status, Valid Until, and Generated By. On the right, there is a 'Search' section with filters for Code, Print Status, Usage Status, and Plan. Below the search filters is a 'Generate' section with fields for Number of Codes and Plan (set to TY5Daytest), and a 'Generate' button. At the bottom, there are buttons for 'Delete Selected', 'Print Selected', and 'Kick Selected'.

Fig 7.3a –hotspot plan and voucher generation

7.4 Overview

Hotspot service can operate as pay service or office access or both.

1) Pay service access

- a) First, create voucher plans for operator to generate voucher easily and quickly.
Both prepaid and postpaid plans can be tailored to a list of parameters such as the following:
 - Maximum time usage,
 - Download/upload speed,
 - Maximum data access
 - Charges per hourMultiple plans can be created for different connection time, charges, etc.combinations.
- b) To generate voucher, operator selects Prepaid or Postpaid option.
Under **Generator** on the right hand side, enter the number of vouchers to be created and select one of the plans.
- c) Operator can monitor and manage user connection status.
Prepaid and Postpaid users list are displayed on separate pages.
If the list is too long, the operator can use search option to quickly retrieve the information.
Operator/Cashier can print out the voucher containing their access code and also control their access duration in the network either by limiting the amount of access time or the amount of data used.

2) Office and Guest access

Hotspot is also applicable in the office environment. Office and Guest plan can be created.
Office and Guess plan setup helps simplify staff and guest account generation.

- a) First select access parameters for the new Office plan.
Available selections are:
 - Maximum time usage
 - Download/upload speed
 - Maximum data access
Under the Guess plan, only the Download/Upload speed parameter can be selected.
- b) Next, the administrator from the Generator page creates the staff and guest accounts.
- c) Manager can monitor and manage staff from the Office and Guest list

For more details on creating plans and user accounts, please refer to the **Hotspot@work Management** document.

* **Hint** : You can install multiple Internet routers to setup broadband aggregation to increase the broadband sharing bandwidth for the hotspot service.
Refer to the section, [Setup Broadband Aggregation on the Mesh Network](#) in this document.

8 Reporting

Report system creation is based on the history of MPs and the client connections.

To view and print the report, click the **Report** tab on the menu. From the **Generate Report** box, first select the starting and ending date and time in the **From** and **To** box. Then click one of the two report format buttons below to generate. See the **Report** tab page in fig 8a below.

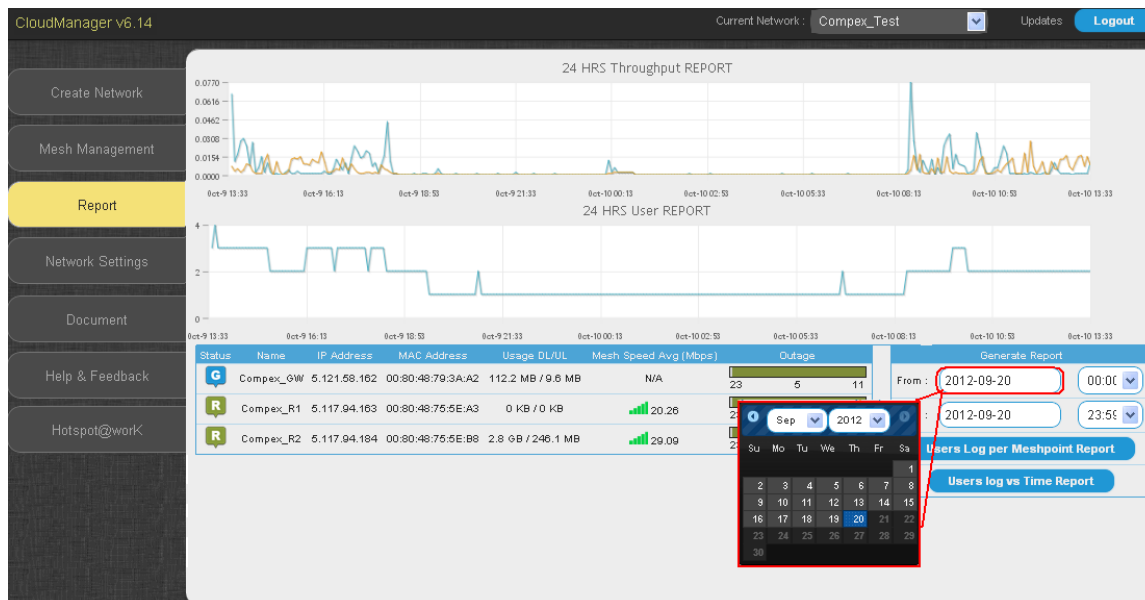


Fig 8a –Report tab page

8.1 Performance Report

In this section, we will analyze MP's performance over time, including the mesh speed and outage for each particular MP. The chart gives an overview of the performance for the last 24 hours.

To generate report of specific date and time (up to one month period) use the **Generate Report** box.

8.1.1 Users Log Per MeshPoint Report

This report shows all the users and the MPs they were connected for the selected period when generating the report. These users are identified by their MAC addresses listed under the **MAC Address** column.

You may notice in the report the same user have connection to two or more MPs.

The RSSI value shows the user's connection signal strength with that MP.

The user might have roamed to other MPs with the higher signal strength (RSSI).

It is normal for report to show multiple users with multiple MPs connections when these conditions listed below are more favorable for roam to occur.

- ✓ The roaming sensitivity level setting is high
- ✓ The MPs are closer to the users

The roaming sensitivity level is set in the **Minimum Signal Strength** parameter of the SSID profile in the **Network Settings** tab page.

MAC Address	MeshPoint	RSSI(last)
00:80:48:68:bb:90	Gateway_RD	37
00:80:48:65:da:15	June	33
00:80:48:65:da:15	Gateway_RD	39
00:80:48:6e:27:45	Gateway_RD	48
00:80:48:6f:81:fa	Gateway_RD	46

Fig 81.1a –Sample "Users Log per MeshPoint"

MAC Address : Display the MAC Address of the user connected to the device.

MeshPoint : Shows the MP name that the user uses.

RSSI (Last) : RSSI of the user when it is last seen. **Green** represents RSSI>20.
Yellow is 10<RSSI<20. **Red** is RSSI<10.

* **Note:** MeshPoint with no user connection will not be displayed.

8.1.2 Users Log vs Time Report

This report shows the users' login and logout time from the respective MPs for the selected period when generating the report. Such report should select at least 24 hours period or 1 day when generating the report.

By tracing the user first occurrence of the start connection time in the **Last Seen On** column starting from top down of the report and then trace from bottom up for the same user first occurrence for the last connection time. This will show the user login and logout time for the day.

MAC Address	Last Seen On	MeshPoint	RSSI(last)
00:80:48:68:bb:90	10-11 10:14	Gateway_RD	36
00:80:48:65:da:15	10-11 12:07	June	33
00:80:48:65:da:15	10-11 13:27	June	34
00:80:48:65:da:15	10-11 13:39	Gateway_RD	42
00:80:48:65:da:15	10-11 13:47	June	33
00:80:48:65:da:15	10-11 13:59	Gateway_RD	41
00:80:48:65:da:15	10-11 14:12	June	34
00:80:48:65:da:15	10-11 14:24	Gateway_RD	39
00:80:48:65:da:15	10-11 14:32	June	33
00:80:48:65:da:15	10-11 15:29	Gateway_RD	38
00:80:48:65:da:15	10-11 15:42	June	33
00:80:48:65:da:15	10-11 16:04	Gateway_RD	40
00:80:48:65:da:15	10-11 16:17	June	34
00:80:48:65:da:15	10-11 16:29	Gateway_RD	39
00:80:48:65:da:15	10-11 16:52	June	33
00:80:48:65:da:15	10-11 17:04	Gateway_RD	41
00:80:48:68:bb:90	10-11 18:19	Gateway_RD	37
00:80:48:6e:27:45	10-11 18:19	Gateway_RD	48
00:80:48:6f:81:fa	10-11 18:19	Gateway_RD	46

Fig 8.1.2a –Sample “Users Log vs Time”

MAC Address : Display the MAC Address of the user connected to the device.

Last Seen On : If it disappears on the network, it will show the time that it is last seen on the network.

MeshPoint : Shows the MP name that the user uses.

RSSI (Last) : RSSI of the user when it was last seen. **Green** represents RSSI>20.
Yellow is 10<RSSI<20. **Red** is RSSI<10.

* **Note:** You would notice that in this report, the same client would be logged into the same MP over a period of time, capturing the check-in and check-out time of the station in the date range specified.

S1 Special Configurations

S1.1 Bridge Mode

When bridge mode is enabled:

- The mesh gateway MP's WAN port will disable the NAT mode and bridge the wireless mesh network with the upstream wire network. Applications that require this include camera video streaming, multiple bridge connections from the wireless mesh network to shared resources on the upstream network.
- All users will obtain their IP addresses from the upstream DHCP server and router.
- Provide VLAN tagging on the WAN port and VLAN ID association to SSID profiles. Applications include network connection security, redirecting of wireless connection with different SSID profiles to different network level security connection on the upstream networks.
- Outbound wireless packets are not VLAN tagged. But inbound wireless packets to the WAN port are VLAN tagged.

Setup examples

S1.1.1 Setup VLAN Tagged over MeshPoint WAN port

When the upstream network uses VLAN tags to connect the networks, wireless mesh network connecting to such network will be required to setup a VLAN tag through its gateway node. Compex wireless mesh network uses the gateway MeshPoint WAN port with bridge mode to make such a connection. Enabling bridge mode displays the VLAN ID setup page. See **Fig 1.1.1a** below.

The screenshot shows the 'Advanced Settings' section of a network configuration interface. A sidebar on the left has 'Network Settings' highlighted. The main area is titled 'Advanced Settings' and contains the following elements:

- Bridge Mode:** A checkbox that is checked.
- WAN VLAN ID:** A dropdown menu set to 'Tagged' and a text box containing the number '2'.
- SSID1 VLAN ID:** A dropdown menu set to 'Untagge'.
- SSID2 VLAN ID:** A dropdown menu set to 'Untagge'.
- Help Text:** A paragraph explaining that bridge mode disables NAT and allows LAN access. It also provides a warning for the WAN VLAN ID setting, stating it's only for the WAN port and that incorrect configuration could lead to a total network loss.
- Buttons:** 'Save Settings' and 'Delete Network' buttons at the bottom.

Fig 1.1.1a –Enable Bridge Mode display VLAN ID setup page

- * **Note:** When you set a VLAN tag and upstream switch is not able to support VLAN tag for the gateway port, you would lose the entire network connection. Proceed with changes only if you are certain of the configuration in your switch.

WAN VLAN ID : This VLAN ID entered is setup on the WAN port of the MeshPoint
To enable the VLAN tag, first select **Tagged** and enter the VLAN ID number in the adjacent box.
To disable VLAN tag, select **Untagged**

SSID1 VLAN ID : This VLAN ID entered is setup to associate with SSID1 profile.
To enable VLAN tag, first select **Tagged** and enter the VLAN ID number in the adjacent box.
To disable VLAN tag, select **Untagged**

SSID2 VLAN ID : This VLAN ID entered is setup to associate with SSID2 profile.
To enable VLAN tag, first select **Tagged** and enter the VLAN ID number in the adjacent box.
To disable VLAN tag, select **Untagged**

- * **Note :** The VLAN ID association to an SSID profile is such that outbound wireless packets are not tagged with a VLAN ID. But inbound wireless packets to the WAN port are tagged with the VLAN ID.

S1.1.2 Multiple gateways using bridge connection to Company LAN network

For medium to large mesh network, connect multiple gateways to LAN shared resources is the best approach. Mesh gateway connection is the recommended solution.

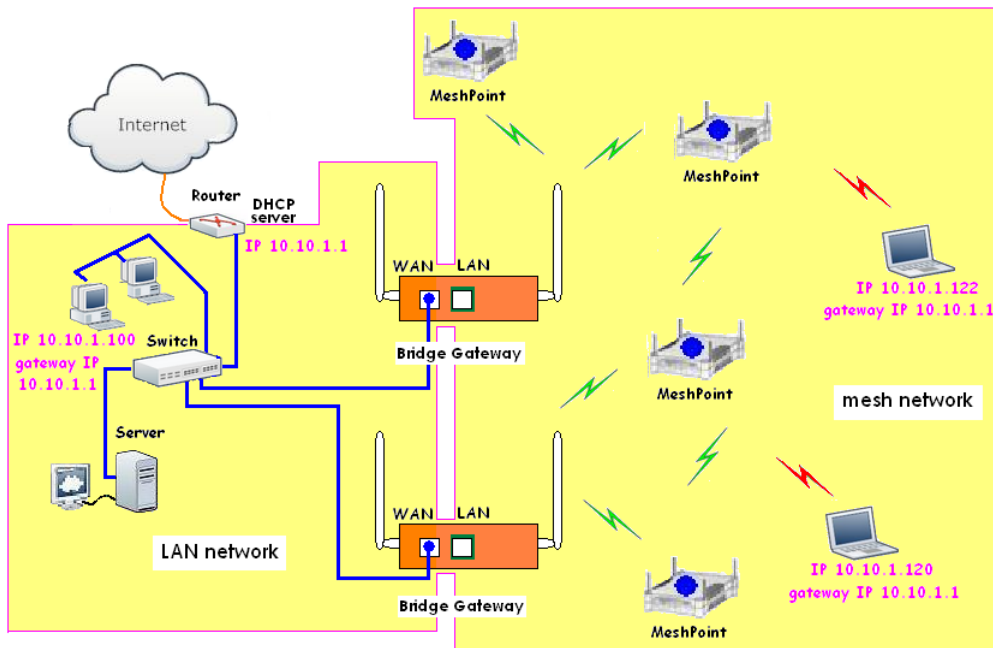
However, in the event when multiple bridge connections must be deployed, Compex recommend the Gateway-Bridge connection mode.

Multiple bridge connections between wired and wireless network can create network loopback. To overcome this Compex MPs implement BATMAN advanced BLA II (bridge loop avoidance) on the WAN port when the Bridge mode is enabled creating a Gateway-Bridge connection mode.

To setup such connection, follow the steps below,

- Gateway MP must use the WAN port for the connection.
- Bridge Mode** must be enabled.
Network Settings tab -> Advanced Settings section -> check the Bridge Mode box.

The diagram below illustrates how the two networks are connected with two bridge connections. As the wireless mesh network and the LAN network are bridged, the Internet router or DHCP server on the LAN network will issue IP addresses to all devices on the LAN and wireless mesh network.



Multiple bridge gateway connections to LAN network.
MeshPoints use WAN port connection with Bridge Mode enabled.

Network Settings tab -> Advanced Settings section -> Bridge Mode ☒

Fig S1.1.2a –Special bridge-gateway connection example

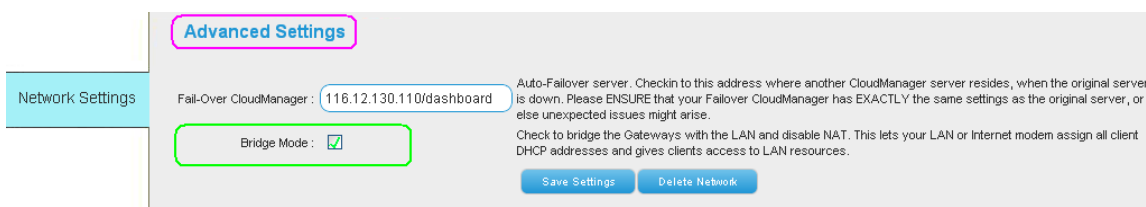



Fig S1.1.2b –Add a check Bridge Mode box to enable bridge-gateway on the WAN port

S1.2 Setting up a Wireless Mesh System without Internet and MeshController

Sometimes, you just wanted a simple mesh system without any controlling mechanism. But you would still need to define a Mesh Gateway, as the main motivation for deploying a mesh system is to create redundancies for the mesh repeaters to go back to the gateway.

How to setup the Mesh Gateway (Follow this to set it up as a non-DHCP client)

1. First run **Add MeshPoint** button and add this MP (designate as the gateway) from the CM. Ensure the MAC address entered is the Wireless Backhaul MAC address.
2. The IP address allocated for the MAC address is stated on the CM (eg. 5.118.205.192)



Status	Name	Description	IP Address	MAC Address	Cu
X	test	test	5.118.205.192	00:80:48:76:CD:C0	

Fig S1.2a –Virtual MC IP address

This is not the IP address for the device itself, but it is derived from that IP address. The IP address for the gateway would be 101.205.192.1, with the circled IP address replacing the XXX.XXX in 101.XXX.XXX.1

3. Set up your PC IP to be a 101.XXX.XXX.10, and in our example would be 101.205.192.10.
4. In your web browser, enter 101.XXX.XXX.1, and in our example would be 101.205.192.1

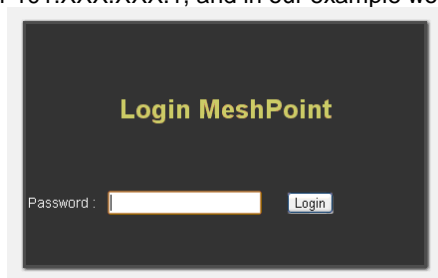


Fig S1.2b –MP login prompt

5. Login with the password (default is 0p3nm35h)
6. Go to “Settings” and at **Local Web Pages**, enable **Internet Test**, as shown below. This would stop the MP from rebooting, if it cannot reach the Internet or the MC.

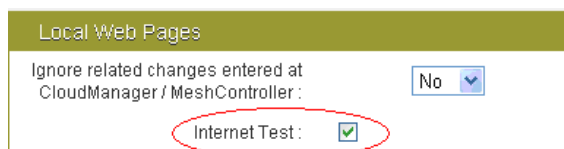


Fig S1.2c –MP Local WebPages

7. At the “Gateway Settings”, choose

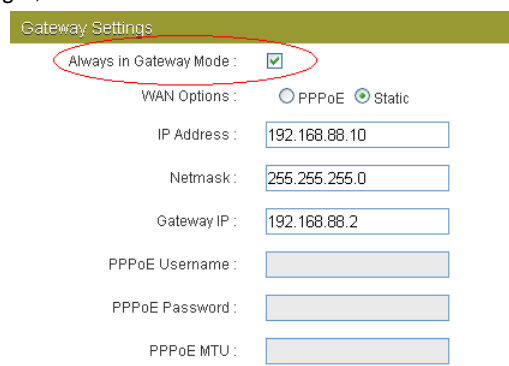


Fig S1.2d –MP Gateway Setting page

8. Click **Save Settings** and then reboot. This would then act as a gateway, regardless of whether there is a DHCP IP or not. Also, you can select PPPoE as a WAN option.
9. NOTE: the four LEDs (red, orange, green, green) will not light up in this setup. In normal situation the four LEDs will light up when the gateway can check-in to the CM or MC. Since there is no Internet connection or MC, they will be no light up.
For repeater, the definition of the four LEDs is different. They indicate the link quality level with the gateway.

How to setup the Repeater

1. There is a DHCP Server at the gateway, and the repeater would be able to get the DHCP IP from the DHCP Server.
2. Once you see the four LEDs (red, orange, green, green) light up, it means that it has connected to the gateway.
3. Connect to the LAN port or use wireless to connect to the Repeater. Then use uConfig to find the Repeater IP Address. The example below shows that it is 101.205.192.10

MP543A	Meshwork	00-80-48-6d-d2-c9	101.205.192.10	##
MP546A	Meshwork	00-80-48-76-cd-be	101.205.192.1	

Fig S1.2e –uConfig scan

4. Double-click on the IP address on the uConfig or enter the 101.205.192.10 in your web browser.

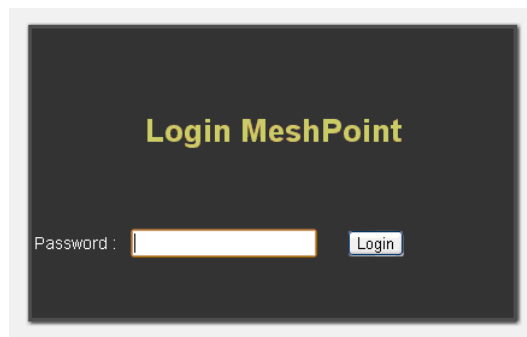


Fig S1.2f –MP login prompt

5. Login with the password (default is Op3nm35h)
6. Go to **Settings** and at **Local Web Pages**, enable **Internet Test**, as shown below. This would stop the MP from rebooting, if it cannot reach the Internet or MC.

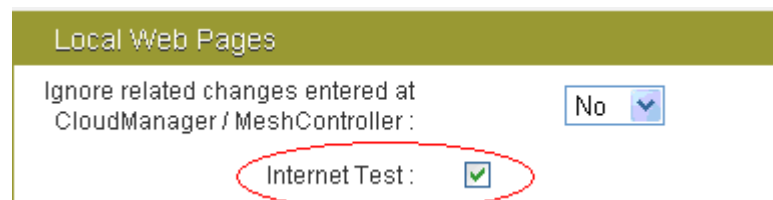


Fig S1.2g –MP Local WebPages

7. Save and reboot.

S1.3 Customizing of individual MeshPoint

You need to customize the individual MP for the following purposes:

- To disable the MP from rebooting when the Internet connection is lost and/or cannot connect to the controller
- To change the MP Coverage Channel to avoid using same or overlapping frequency with neighbor MPs
- To set channel bonding to a small group of MPs in the mesh network that have favorable conditions to achieve better performance
- To adjust the MP Transmit Power such that the signal strength in the area it covers does not appear to be stronger than its neighbor MPs to their neighbor clients
- To enable or disable the MP from doing automatic firmware update
- To set a different SSH password for the MP

To customize the settings of an MP, from the CC, open the **Mesh Management tab page** from the menu. Click the **Edit button** for that MP in the MP list table you want to edit. The **Edit MeshPoint page** below displays.

Edit MeshPoint

MeshPoint Name : Only "A-Z", "a-z", "_", "-" (underline), "-" (dash) and "0-9" are allowed.

MAC Address :

MeshPoint Description :

No Reboot if no Controller : If this is not enabled, this MeshPoint would reboot, if there is no route to Internet CloudManager or MeshController.

Transmit Power : The transmit power is only for coverage radio and is the same for all SSIDs on this MeshPoint. For MPE72 and MP546G, as the backhaul radio is the same as coverage radio, it would change the backhaul area too if you change the transmit power.

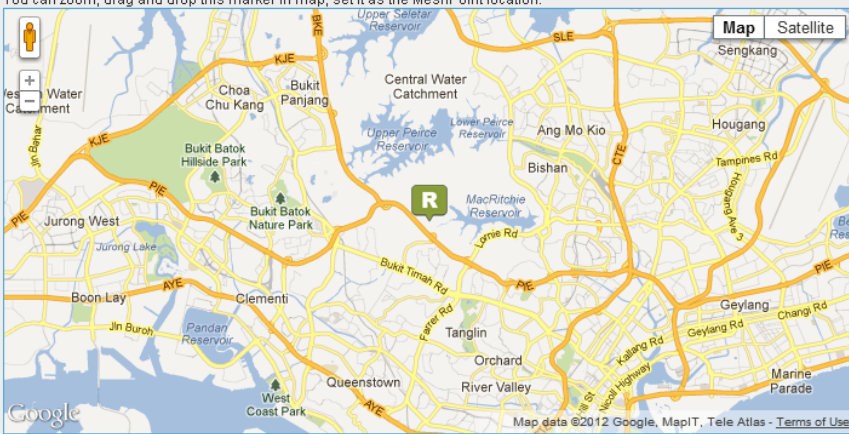
SSH Passwords : If set it as empty, means to use the network settings.

Freeze Firmware : Freeze the firmware version to prevent auto-upgrade of new firmware.

Channel Spectrum Width : Channel Spectrum Width for Coverage channel. For MPE72 and MP546G, as the backhaul radio is the same as coverage radio, it would change the backhaul Channel Spectrum Width too, if you change the Channel Spectrum width.

Coverage Channel : Channel for coverage(SSID1/SSID2).

Location : You can zoom, drag and drop this marker in map, set it as the MeshPoint location.



Latitude : 1.3439102333574835 Longitude : 103.8053834438324

Fig S1.3 –Edit MeshPoint page

No Reboot if no Controller : In a standard network setup the MP will check-in once every 5 minutes to the controller. If it fails to check-in it could mean MP has lost the connection and will automatically reboot to recover. However, the situation could be just the Internet connection is lost and you do not want this MP to reboot. You then set to **Enable**.

** **Note:** If you don't use a controller for your network, skip this option. Use the Network Settings tab page global setting.*

Options are: **Use Network Setting**, **Enable**, and **Disable**

Select **Enable** will prevent this MP from rebooting.

Select **Disable** will ensure this MP will always reboot.

Using global setting, select the default, **Use Network Setting**.

** **Note:** When set to **Enable** or **Disable**, it overrides the global setup in the **Network Settings** tab page.*

Transmit Power

: This setting lets you adjust this MP coverage radio transmit power so its signal strength won't appear to be stronger than neighbor MPs to their neighbor clients to achieve a more balance connections over the MPs and better roaming experience.

Adjustment can be set lower in one dBm steps.

Using global setting, select the default, **Use Network Setting**.

** **Note:** For Single Radio MP, adjusting the coverage radio transmit power also set the backhaul transmit power.*

SSH Password

: Leave it blank to use the global password setting for all the MPs. Enter a new password in the box if this MP must use a different password.

Freeze Version

: This setting flag to allow or disallow this MP to do firmware upgrade.

Select **Enable** to disallowed automatic firmware update on the MP.

Select **Disable** to always allow automatically firmware upgrade on the MP when there is newer firmware.

When **Enable** or **Disable** is selected it overrides the global setting.

Using global setting, select the default, **Use Network Setting**.

Channel Spectrum Width

: This setting lets you select the 11n channel transmission width for this MP between the normal 20MHz or 20/40MHz (channel bonding). Options are: **11ng20**, **11na20**, **11na**, **11ng**, **Use Network Setting**.

- **11ng20** selects **2.4GHz** band for 11n with **20MHz** channel width.
- **11ng** selects **2.4GHz** band for 11n with **20/40MHz** channel width.
- **11na20** selects **5GHz** band for 11n with **20MHz** channel width.
- **11na** selects **5GHz** band for 11n with **20/40MHz** channel width.

Using global setting, select the default, **Use Network Setting**.

Coverage Channel

: This setting lets you select a different coverage channel to avoid using same or overlapping channel with nearby MPs.

Non-overlapping channels for 2.4GHz band are Channel1, Channel 6 and Channel 11.


To select, click on the channel number, range 1 to 11 or 1 to 13, depending on the country set selected.

When **Auto** is selected, the channel is automatically selected during the initial power up sequence.

** **Note:** For Single Radio MP, there is no Auto selection.*

Using global setting, select the default, **Use Network Setting**.

Location

: Google Map will be displayed in this box when the **World Map** is selected. You can drag the marker  over the map to show this MP location.

The Latitude and Longitude show the global positioning of the MP if **Custom Map** is selected and no map is uploaded, the box will display the marker only.

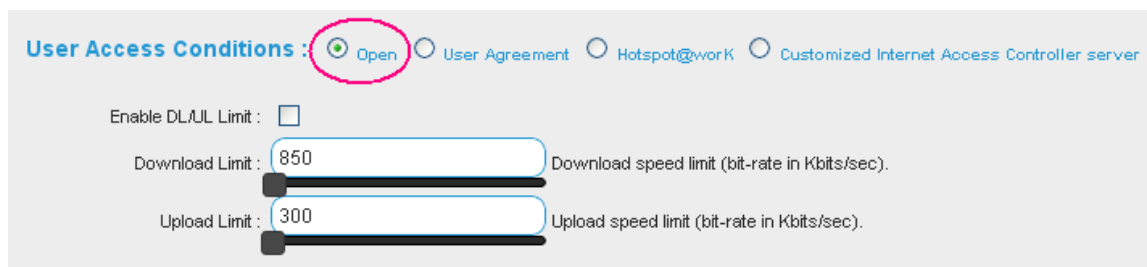
To upload the map, use the Upload Map option at the top of the page. Click the **Choose File** button to browse and select the map file from your PC hard drive. Then click the **Upload Map** button to start the file upload. Drag the marker over the map to place the MP. The X-axis and Y-axis show the MP position on the map.

A1 APPENDIX I

A1.1 Users Access Conditions

There are 4 different methods for Integrators to control how users access on the network. They are **Open**, **User Agreement**, **Hotspot@work**, **Customized**, and **Internet Access Controller**. You can set them under the **Network Settings** tab page, in the **Advanced Settings** section.

A1.2 Open

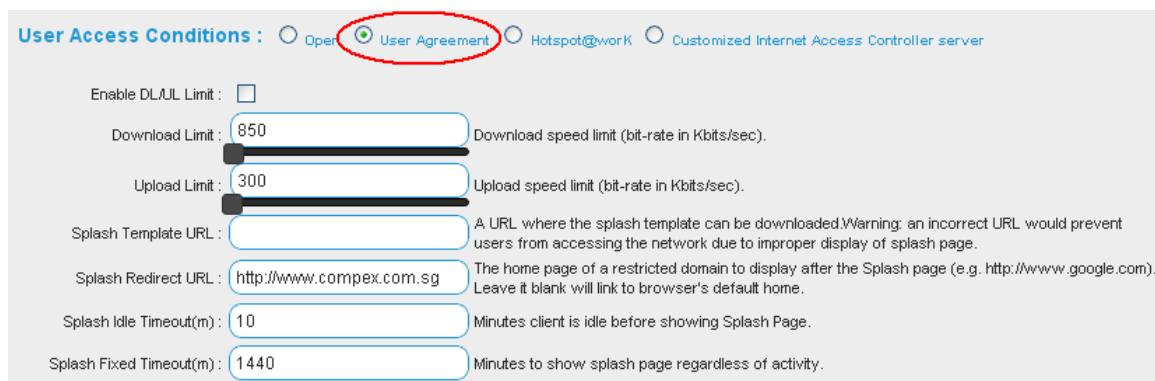


The screenshot shows the 'User Access Conditions' configuration page. At the top, there are four radio button options: 'Open', 'User Agreement', 'Hotspot@work', and 'Customized Internet Access Controller server'. The 'Open' option is selected and circled in pink. Below the options, there is a checkbox for 'Enable DL/UL Limit' which is unchecked. Underneath, there are two input fields: 'Download Limit' with a value of 850 and 'Upload Limit' with a value of 300. To the right of each input field is a slider bar and a text description: 'Download speed limit (bit-rate in Kbits/sec)' and 'Upload speed limit (bit-rate in Kbits/sec)' respectively.

Fig A1.2a –Selecting the Open option

Users are allowed to use the network with no restrictions. Integrators however can set the download and upload speed limit per MP, not allowing each coverage area of the MP to hog the network. Entries in the download and upload limiting boxes are in kilobits per second (kbps).

A1.3 User Agreement



The screenshot shows the 'User Access Conditions' configuration page with the 'User Agreement' option selected and circled in red. The 'Enable DL/UL Limit' checkbox is unchecked. The 'Download Limit' is set to 850 and the 'Upload Limit' is set to 300. Below these are four more input fields: 'Splash Template URL' (with a warning note), 'Splash Redirect URL' (with an example URL), 'Splash Idle Timeout(m)' (set to 10), and 'Splash Fixed Timeout(m)' (set to 1440). Each of these fields has a corresponding text description to its right.

Fig A1.3a –Selecting the User Agreement option

Users are required to enter a splash page and authenticate a network. Integrators can set the download and upload speed limit per MP, not allowing each coverage area of the MP to hog the network. A different splash page can be pre-determined as well, giving more variety to the users. Users can be re-directed to a webpage of the Integrator's choice, giving the Integrators more opportunities to advertise their products. The splash idle and fixed timeout can be set as well, making sure that more users are able to see the captive portal.



Fig A1.3b –Splash Page (Compex Default)

Note:

For customers who want to do their own splash pages, please note the following:

1. Each individual file has to be <100KB.
2. The total size for all the files has to be <300KB.
3. The files have to be arranged in the right folders. Please check the package issued by Compex.
4. References to images need to have double quotes. Please refer to the example in the package.

A1.4 Hotspot@work

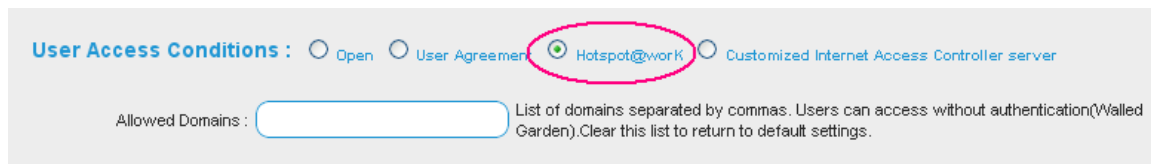


Fig A1.4a –Selecting the Hotspot@work option

This selection enables the Hotspot services. It includes hotspot billing services and Office/Guest access. Using Radius Server to authenticate users, integrators are able to release username and password to the customers. They will be able to either charge users to enhance their profits or be able to control their Internet usage.

- * **Note:** Access Policies and Users accounts can be setup in the Hotspot Management by hotspot manager. First, Hotspot@work must be enabled, then you can display the Hotspot@work tab page to create hotspot the manager accounts.

The **Allowed Domain box** allows integrator to provide free connections to specific web pages and web sites to users without logging to hotspot.
Enter all the website addresses selected for free access in the **Allowed Domains box**.

A1.5 Customized Internet Access Controller

Will be available soon.

A2 APPENDIX II

A2.1 Connecting to the existing network

Like single AP networks, the wireless mesh network needs to connect to the existing network using shared resources.

Unlike single AP networks, the wireless mesh network can have single and multiple connections.

A2.2 Scenario 1: Using WAN port to connect to company's existing network

When the MeshPoint connects its WAN port, the existing network must have an Internet router.

It becomes a **mesh gateway** after obtaining an IP address at its WAN port. NAT is enabled.

Wireless mesh network can have one or several such mesh gateway connections.

You connect multiple mesh gateways for the following reasons.

- i) To avoid single point connection failure with shared resources.
- ii) To reduce the number of mesh hops for medium to large networks.

There is no required change to the existing network configuration. PCs, in the existing network continue to operate as before. Users connected to the wireless mesh network will immediately be able to access both the Internet and existing network resources, such as, servers and printers.

This is the recommended connection.

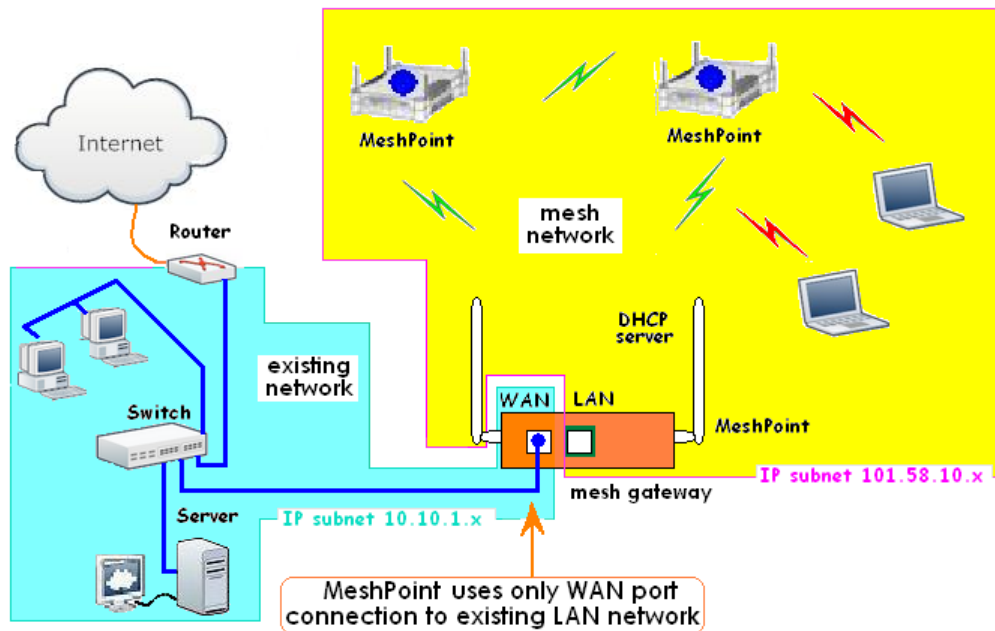


Fig A2.2a –Mesh Gateway example

A2.3 Scenario 2: Using LAN port to connect to company's existing network

An MP when connecting its LAN port to an existing network, creates a bridge connection between the wireless mesh network and the existing network. This MP becomes a mesh bridge between wireless mesh network and existing network. See **Fig A2.3a** below

Both wireless and PC users obtained their IP addresses from the Internet router directly.

Only one mesh bridge connection from wireless mesh network to existing network is supported.

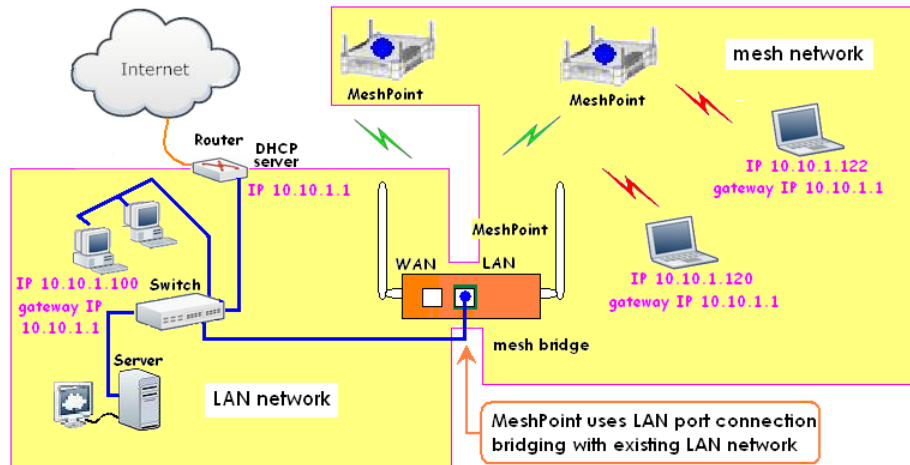


Fig A2.3a –Gateway using LAN port connection example

* **Note:** Currently, only one mesh bridge connection is supported.
If multiple connections are needed, use the WAN port instead.
Please refer to [Special Configuration](#) section.

A2.4 Scenario 3: Using both WAN and LAN ports to connect to existing network

This is a more complex setup connection. Some **changes to the existing network resource configuration will be required**. You only setup such connection when you must have **wireless mesh and existing network to be on the same IP subnet**. See Fig A2.4a below.

When the MP connects to both WAN and LAN ports, the WAN port must be connected only to the Internet router. The Internet router needs to be disconnected from the existing network and its configurations; IP address setup needs to be changed. The MP then becomes a mesh gateway. Both wireless and PC (on existing network) users obtained their IP addresses from this mesh gateway. When wireless and PC users access the Internet, traffic is routed from the WAN port of the mesh gateway to the Internet router.

Next, the MP LAN port connects to the existing network switch. This creates a bridge connection between the wireless mesh network and existing network. Wireless users that access to the company resources such as server and printer passes through this LAN port.

Multiple mesh gateways connecting to the existing network is supported.

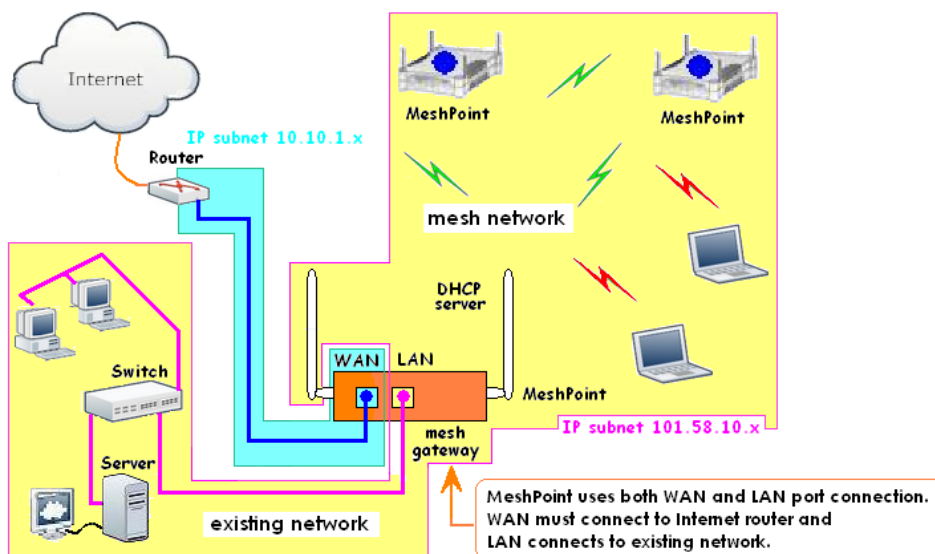


Fig A2.4a –Example: Gateway with WAN and LAN port connection

A3 APPENDIX III

A3.1 How to add MeshPoints using Import File method

This section explains how to create an import file in text format for uploading the MPs to the CC. Below is a sample of the data format.

**** Note: Sample file in excel format is for show only. Excel format CANNOT be used to upload. File must be in text format.**

*** Hint :** If you create the Import file using Excel, remember to save a copy in text format before using it to do the Import MP upload.

How to creating the text format file.

	A	B	C	D	E	F
1	Name	Description	MAC_Address	Span_Name	Latitude	Longitude
2	meshpoint_name	meshpoint_description	00:80:48:11:11:11			
3	span_name	span_description		span_name	1.000000	2.000000
4	meshpoint_name_span	meshpoint_description	00:80:48:11:11:12	span_name	1.000000	2.000000
5						

Fig A3.1a –Import file data format

Rules for creating the text file according to the following data format.

To create import file for MPs, refer to Fig A3.1a above on item 1 and 2.

- First line should contain the header, **Name**, **Description**, **MAC_Address**
- **Latitude** and **Longitude** entries are optional. Need not include in file if not used.
- All names and descriptions field cannot have a space. Use the underline character instead.
- For proper display, keep description as short as possible (not more than 20 chars).
- Each field must be separated by one tab only. Use two tabs to skip a field.
- MAC address must be of the format, XX:XX:XX:XX:XX:XX

*** Note, In the examples below, the tabs between fields are spaced out just for illustration only. In the actual import file there should be no spaces between the tabs. .**

Example 1

```
Name <tab> Description <tab> MAC_Address
AP1 <tab> In_the_hall <tab> 00:80:48:11:22:33
```

In example 1, **Span_Name**, **Latitude** and **Longitude** info are not required, and **MAC_Address** is the last item. Thus, there is no need to add tabs after the **MAC_Address** field.

In example 2 below, to skip the **Span_Name** field, two tabs are used.

There should not have any space between the two tabs.

Example 2 includes latitude and longitude position info.

```
Name <tab> Description <tab> MAC_Address <tab> Span_Name <tab> Lati <tab> Long
AP1 <tab> At_Bldg_A <tab> 00:80:48:11:22:33 <tab><tab> 1.40 <tab> 103.80
AP2 <tab> At_Bldg_B <tab> 00:80:48:11:22:35 <tab><tab> 1.409 <tab> 103.8005
```

In example 2, **Span_Name** is not used. But there are **Latitude** and **Longitude** info. So there must be 2 tabs for **Span_Name** item to skip that field then followed by the **Latitude** and **Longitude** info.

To upload text file, click the **Import MeshPoints** button see **fig 4.2c** (Ch 4), choose the file and click the **Import** button to start uploading the file.

End of instruction.

A3.2 How to add MeshPods using Import File method

This section explains how to create an import file in text format for uploading the MPods to the CC.

**** Note: Sample file in excel format is for show only. Excel format CANNOT be used to upload. File must be in text format.**

*** Hint :** If you create the Import file using Excel, remember to save a copy in text format before using it to do the Import MP upload.

	A	B	C	D	E	F
1	Name	Description	MAC_Address	Span_Name	Latitude	Longitude
2	meshpoint_name	meshpoint_description	00:80:48:11:11:11			
3	span_name	span_description		span_name	1.000000	2.000000
4	meshpoint_name_span	meshpoint_description	00:80:48:11:11:12	span_name	1.000000	2.000000
5						

Fig A3.2a –Import file data format

Rules to create the text file of the following data format.

To create import file for MPods, refer to **Fig A3.2a** above on item 3 and 4.

- First line should contain the header, **Span_Name**, **Span_Description**, , **Span_Name**
- **Latitude** and **Longitude** entries are optional and can be excluded from the file if not in use.
- **Name** field cannot have a space. **Description** can have a space between words.
- For proper display, keep description as short as possible (not more than 20 chars).
- Each field must be separated by tab. Use 2 tabs to skip a field.
- MAC address must be of the format, xx:xx:xx:xx:xx:xx

The first line creates the **Span_name**. So leave the MAC address field blank by adding two tabs. Add MPod and its MAC address starts from the second line onwards.

*** Note, in the examples below, the tabs between fields were spaced out just for illustration only. In actual import file there should be no spaces between the tabs.**

To skip a field, use two tabs. There should not have any space between the two tabs.

Example 1

```

Name <tab> Description <tab> MAC_Address <tab> Span_Name
Span-A <tab> at_building_A <tab><tab> Span-A
Mpod1 <tab> at_MSpan_nodeA <tab> 00:80:48:aa:bb:cc <tab> Span-A
Mpod2 <tab> at_MSpan_nodeA <tab> 00:80:48:aa:bb:cd <tab> Span-A
Span-B <tab> at_building_B <tab><tab> Span-B
Mpod3 <tab> at_MSpan_nodeB <tab> 00:80:48:ee:ff:00 <tab> Span-B
Mpod4 <tab> at_MSpan_nodeB <tab> 00:80:48:ee:ff:01 <tab> Span-B

```

To upload text file, click the **Import MeshPoints** button see **fig 4.2c** (Ch 4), choose the file and click the **Import** button to start uploading the file.

End of instruction.

M1 System tools

M1.1 Changing the MeshController IP Address

The MC factory default IP address is 192.168.0.2

You will need to change the IP address when installing the MC to your network of a different IP address. Follow the instruction below to make the change:

Open the web browser and connect to the MC by typing the URL, <http://192.168.0.2>

Type your MC IP address, if different, to login.

Login with the default **User Name**, admin and **Password**, password.

Use your user name and password, if different.

Click the **System** tab on the menu.

*** Note :** *Each section have its own Save Settings button. Only changes made in that section is saved.*

Fig M1.1a –Changing MeshController IP setup

*** Note:** Remember to change your PC IP address when connecting to the MC after reboot.

M1.2 Setting the NTP server on MeshController

MC and MP devices uses the NTP server to maintain accurate date and time.

Follow the instruction below to add new NTP servers.

Open the web browser and connect to the MC by typing the URL, <http://192.168.0.2>

Type your MC IP address, if different, to login.

Login with the default **User Name**, admin and **Password**, password.

Use your user name and password, if different.

Type the new NTP server in the **Add NTP Server box** and click the **Add button**.

Entry can be the domain name or the IP address of the NTP server.

At least 2 NTP server entries is recommended.

Priority is from top to bottom. If there is no respond from the NTP server, the next one down the list will be use to get the date and time.

Fig M1.2a –Adding NTP servers

M1.3 Instructions on Resetting the MeshController

The procedures below describe how to reset the MC device to factory defaults.

MC (with firmware B1076) can be reset using the software reset (from webpage) and hardware reset buttons.

- **Caution: Reset will clear all data in the MC and return it to the factory defaults. All data will be lost.**

Hardware reset

After you press for >6 seconds and then release, the LED would start to blink from left to right (red to green) continuously. Then it would reboot after 30 seconds. Once it is up, the MC is reset.

Software reset (from the webpage)

After you press the reset button on the **System** tab page, and you will be prompted to reset the controller.

Press **No** to cancel. Press **Yes** to proceed.

After you press **Yes**, the LEDs start to blink from left to right (red to green) continuously. Then it would reboot after 30 seconds. Once it is up and running again, the MC is reset.

- ** Note:** After MC is reset, the IP address will revert to factory default. Remember to changed your PC IP address to the same default IP subnet to be able to reconnect with the MC again.

End of procedure.

M1.4 How to manually update a MeshController firmware

The procedures below describe how to manually upgrade the MC to a newer firmware.

Step 1

First enter the path name in the **Firmware Server** box where the firmware image file will be found. See the **blue** arrow in the **fig M1.4a** below.

The screenshot shows the 'Advanced Settings' page of the MeshController web interface. On the left, there is a sidebar with 'Network Settings' highlighted. The main content area contains various configuration options. A blue arrow points from the left towards the 'Firmware Server' field, which is highlighted with a purple box. The 'Firmware Server' field contains the text 'my_dashboard/dashboard/firmw'. Other fields include 'No Reboot if no Controller', 'Transmit Power', 'SSH Passwords', 'Freeze Firmware', 'SSID1 Isolation', 'SSID2 Isolation', 'Country', 'Models in network', 'Mesh Channel', 'Channel Spectrum Width', 'Coverage Channel', 'Fail-Over CloudManager', and 'Bridge Mode'. Each field has a corresponding description or warning on the right side of the page.

Fig M1.4a –Setup Firmware Server path

Remove the tick in **Freeze Firmware box**. Then enter the path name in the **Firmware Server box**. Recommend to use the default path name, **my.dashboard/dashboard/firmware/**
Click the **Save Settings button** to save the changes.

Step 2

Next upload the firmware image file to the MC.

Open the **System tab page**. in the **MeshController Firmware Upgrade section**, click the **Choose File** button to open the computer file browser and locate the new MC firmware file. Refer to the red arrow in the **fig M1.4b** below.

Next, click the **Upload button** to start the file upload.

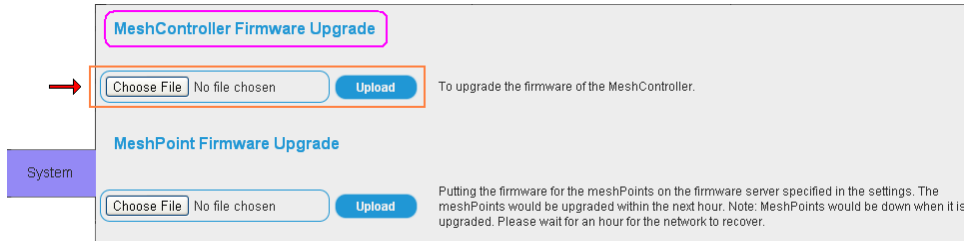


Fig M1.4b –MeshController firmware upgrade on the System tab

Step 3

Run TFTP to write the firmware image file flash.

There are 2 methods. Method (a) is recommended.

For method (b), you may need to try several times to get the timing right to be successful.

a) Using the Reset button method.

- 1) Connect the Ethernet cable to the LAN port of the MC and the PC.
- 2) Press and hold down the **Reset** button of MC, then power on MC.
When diagnostic (Diag) LED starts blinking, release the **Reset** button.
- 3) At the PC command prompt, run the tftp command,
tftp -i 192.168.168.1 put <file name.img>
- 4) The Diag LED light will continue to blink while the file is transferring.
Once the Diag LED light starts to blink slowly, it means file transfer has completed.
- 5) Power off and on MC. When it starts up again it will be running the new firmware.

b) Use this alternative method when the Reset button is not accessible.

- 1) Connect the Ethernet cable to the LAN port of the MC and the PC.
- 2) At the PC command prompt, type the tftp command,
tftp -i 192.168.168.1 put <file name.img>
** Do not press **Return** key on the keyboard yet.
- 3) Power on the MC and wait for 3 seconds for tftp server to start.
After 3 seconds, immediately press the Return key on the PC keyboard to execute the tftp command. It will not work if you run the tftp command after 7 seconds.
* **Note:** The tftp server only waits for 4 seconds. If no valid tftp command is received, it will close and proceed with the boot process.
- 4) The Diag LED light will start blinking and continue to blink while file is transferring.
Once the Diag LED light starts to blink slowly, it means file transfer has completed.
- 5) Power off and on the MC. When it starts up again the new firmware will be running.

End of procedure.

M1.5 How to manually update a MeshPoint firmware

The procedures below describe how to manually upload firmware to a single MP.

Step 1

First enter the path name in the **Firmware Server** box where the firmware image file will be found. See the blue arrow in **fig M1.5a** below.

The screenshot shows the 'Advanced Settings' window of a MeshPoint. A blue arrow points to the 'Firmware Server' field, which is highlighted with a red box. The field contains the text 'my_dashboard/dashboard/firmw'. To the left of the window, there is a 'Network Settings' tab. The 'Freeze Firmware' checkbox is unchecked. The 'Save Settings' button is at the bottom right of the window.

Fig M1.5a –Setup Firmware Server path

Remove the tick in **Freeze Firmware** box. Then enter the path name in the **Firmware Server** box. The firmware image file is generally saved in your PC folder. First make that folder sharable in Windows. Assuming the MP IP is 192.168.168.1 and the PC IP address is 192.168.168.100 and the shared folder name is MP-Firmware. Then, the path name to be entered will be, [\\192.168.168.100\MP-Firmware\](#)

Click **Save Settings** button to save the changes.

Step 2

Run TFTP to write the firmware image file flash.

There are 2 methods. Method (a) is recommended.

For method (b), you may need to try several times to get the timing right to be successful.

a) Using the **Reset** button method.

- 1) i) For **MPE72** connect the Ethernet cable to the **WAN port** of the MP.
ii) For **MP546** connect the Ethernet cable to the **LAN port** of the MP.
- 2) Press and hold down the **Reset** button of MP, then power on the MP.
- 3) When Diag LED starts blinking, release reset button.
- 4) At the PC command prompt, run the tftp command,
tftp -i 192.168.168.1 put <file name.img>
- 5) The Diag LED light will continue to blink while the file is transferring.
Once the Diag LED light starts to blink slowly, it means file transfer has completed.
- 6) Power off and on the MP. When it starts up again the new firmware will be running.

b) Use this alternative method when the **Reset** button is not accessible.

- 1) Same as (a)
- 2) At the PC command prompt, type the tftp command,
tftp -i 192.168.168.1 put <file name.img>

**** Do not press Return key on the keyboard yet.**

- 3) Power on the MP and wait for 3 seconds for tftp server to start.
- 4) After 3 seconds, immediately press the **Return** key on the PC keyboard to execute
- 5) the tftp command. It will not work if you run the tftp command after 7 seconds.

Note: The tftp server only waits for 4 seconds. If no valid tftp command is received, it will close and proceed with the boot process.

- 6) The LED light will start blinking and continue to blink while file is transferring.
- 7) Once the LED light starts to blink slowly, it means file transfer has completed.
- 8) Power off and on MC. When it starts up again the new firmware will be running.

End of procedure.

M1.6 Installer Tools (Only on CloudManager)

Installer Tools is only accessible on the CM.
Currently the following services are supported.

- Changing of MP **Check-In IP** address
- Changing of MP **Mesh ID**

M1.6.1 Changing MP Check-In IP Address

Check-In IP address is the IP address of the host, running the management application, that MP sends the update report every 5 minutes. The host can be the Compex CloudManager (CM) or the MeshController (MC).

For example, if the MC has changed to a new IP address, say, from 192.168.1.10 to the new IP 192.168.1.20, the MPs of the wireless mesh network, hosted by this MC, will no longer be able to check-in to the MC. They must also change their Check-In IP to this new IP address.

The procedure below shows how to run the **Installer Tools** to change the MPs Check-In IP address.

Before you proceed, prepare the following:

- ✓ First, check the MC has configured the **Fail-over-CloudManager** to the address, 116.12.130.110/dashboard
- ✓ Second, check the wireless mesh network is connected to the Internet
- ✓ Third, disconnect the MC from the wireless mesh network after completing step 1

Then execute the procedures below.

Step 1

Check the **Fail-over-CloudManager** has the default address, 116.12.130.110/dashboard
Connect to the MC, open the **Network Settings** tab page, select the **Fail-over-CloudManager** setting in the **Advanced Settings** section. If the **Fail-over-CloudManager** box has a different address, changed it to the CM default address, 116.12.130.110/dashboard and click the **Save Settings** button to save the change.

Then disconnect the MC from the wireless mesh network.

The wireless mesh network should be connected to the Internet at all times.

Step 2

Connect to the CCM using the address, <http://116.12.130.110/dashboard>

Register as a new user. Then enter the user name and password in the **Sign-in** prompt.

Click the **Installer Tools** option to login instead. See the **red circle** in **Fig M1.6.1a** below.



Fig M1.6.1a –CloudManager Sign-In Prompt

After login, you will be prompt to create a new network. Enter a new network name.

Step 3

Next, select the **MeshController IP Addr** tab from the menu.
Enter in the **MAC Address** box, the MP's Wireless Backhaul MAC Address.
Then click **Add MeshPoint** button to add to the list.
If there is more than one MP, repeat the step to enter each one into the table.

MeshController IP Addr

Important Note: Please do not put the MeshController on the network which your MeshPoints can access first. You would need to configure your MeshPoints first.

MAC Address	Checkin IP Address	Fail-Over IP Address	Status	
00:80:48:73:D2:5F	192.168.1.10	116.12.130.110		Delete
00:80:48:6E:C0:43	192.168.1.10	116.12.130.110		Delete

Mac Address: Add MeshPoint

Fig M1.6.1b –Add MP in MC IP Addr tab

Step 4

When an MP has checked-in to this new network in the CM, the four LEDs on that MP will light up. At the same time in the table, the 1st status indicator in the **Status** column, for that MP will turn **orange** color. It will stay in **orange** color when all MPs have not checked-in. See Fig 1.6.1c below.

MeshController IP Addr

Important Note: Please do not put the MeshController on the network which your MeshPoints can access first. You would need to configure your MeshPoints first.

MAC Address	Checkin IP Address	Fail-Over IP Address	Status	
00:80:48:73:D2:5F	192.168.1.10	116.12.130.110		Delete
00:80:48:6E:C0:43	192.168.1.10	116.12.130.110		Delete

Mac Address: Add MeshPoint

Fig M1.6.1c –Status when all MPs have not checked-in to CC

Wait about 10 minutes, once all the MPs have checked-in, the 1st status indicator will turn **green** color, and the **Change Check-In IP Address** button will appear (see Fig M1.6.1d).

Now click the **Change Check-In IP Address** button and enter the new Check-In IP address 192.168.1.20 (i.e. MC's new IP address for this example).

MeshController IP Addr

Important Note: Please do not put the MeshController on the network which your MeshPoints can access first. You would need to configure your MeshPoints first.

MAC Address	Checkin IP Address	Fail-Over IP Address	Status	
00:80:48:73:D2:5F	192.168.1.10	116.12.130.110		Delete
00:80:48:6E:C0:43	192.168.1.10	116.12.130.110		Delete

Change Check-In IP Address Mac Address: Add MeshPoint

Fig M1.6.1d –Status after all MPs have checked-in to CC

Step 5

When an MP has updated to the new Check-In IP address, the 2nd status indicator of that MP will turn **orange** color. It will remain in **orange** color when all the MPs have not updated the new Check-In IP address. See Fig M1.6.1e below.

MeshController IP Addr

Important Note: Please do not put the MeshController on the network which your MeshPoints can access first. You would need to configure your MeshPoints first.

MAC Address	Checkin IP Address	Fail-Over IP Address	Status	
00:80:48:73:D2:5F	192.168.1.20	116.12.130.110		Delete
00:80:48:6E:C0:43	192.168.1.10	116.12.130.110		Delete

Change Check-In IP Address Mac Address: Add MeshPoint

Fig M1.6.1e –Status when all MPs have not updated the new Check-In IP address

In about 10 minutes, once all the MPs have updated to the new Check-In IP address, the 2nd status indicator will changed from **orange** to **green** color. Both 1st and 2nd status indicators will now display **green** color and all the MPs will display the new IP address at the **Check-In IP Address** column in the table. See Fig M1.6.1f below.

This indicates all the MPs have successfully updated the new Check-In IP address.

MeshController IP Add

Current Check-in IP Address:

Important Note: Please do not put the MeshController on the network which your MeshPoints can access first. You would need to configure your MeshPoints first.

MAC Address	Checkin IP Address	Fail-Over IP Address	Status	
00:80:48:73:D2:5F	192.168.1.20	116.12.130.110		Delete
00:80:48:6E:C0:43	192.168.1.20	116.12.130.110		Delete

Change Check-in IP Address

Mac Address :

Add MeshPoint

Fig M1.6.1f –Status after all MPs have updated the new Check-In IP address

Step 6

The prompt, shown below, then display. See **Fig M1.6.1g**.

Complete the process by clicking the **Delete Network (Recommend)** button to delete the temporary network profile.

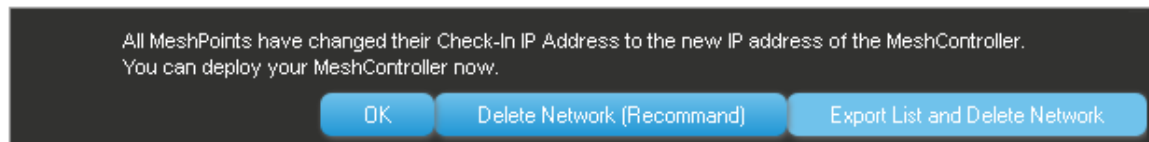


Fig M1.6.1g –Check-In IP Process Final Action Prompt

Export List and Delete Network : Click this button will export the list containing those MPs from this temporary network, if you plan to keep the list.
At the same time, this temporary network profile is deleted.

Delete Network (Recommend) : Click the button to delete this temporary network profile.
This is the recommended action.

OK : Avoid this button unless you plan to keep this temporary network profile to run the process again in the next few days.
Always delete all unused networks.

Process is now completed.

Now, connect the MC to your PC and change to this new IP address 192.168.1.20 and connect the MC back to the wireless mesh network.

All the MPs should now be able to check-in to the MC with the new IP address.

M1.6.2 Changing MP Mesh ID

Mesh ID is the backhaul wireless ID. Every MP is using the same BSSID to connect to each other. You can however change the **Mesh ID** for a group of MPs to forms a smaller isolated wireless mesh network. For example, in the Office, the R&D and Sales departments are just next door and you want to create two isolated wireless mesh networks, one for each department. Both will not communicate over wireless with the other. Thus, R&D and Sales department must use different **Mesh ID** for the MPs.
In this example, you only need to change the **Mesh ID** for one department, say, R&D department.

Before you proceed, prepare the following:

- ✓ The MPs for R&D department must be taken down from the network to change the **Mesh ID**
- ✓ Each MP must connect with the Ethernet cable on the WAN port to the Internet
- ✓ All MPs can simultaneously do the **Mesh ID** update by connecting them to the same switch that connects to the Internet
- ✓ Disconnect the MC from the wireless mesh network after completed step 1

Then execute the procedures below.

Step 1

First check, the **Fail-over-CloudManager box** has the default address, 116.12.130.110/dashboard. Connect to the MC, select the **Network Settings** tab and find the **Fail-over-CloudManager** setting in the **Advanced Settings** section. If the box has a different address, change it to the CM default address, 116.12.130.110/dashboard. Click the **Save Settings** button to save the change.

Then disconnect the MC from the wireless mesh network.

The wireless mesh network should be connected to the Internet at all times.

Step 2

Connect to the CM using the address, <http://116.12.130.110/dashboard>

Register as a new user. Then enter a user name and password and click the **Installer Tools** option to login instead. See the **red circle** in **Fig M1.6.2a** below.



The screenshot shows the 'Sign into CloudManager v6.15' login page. It includes a language selector (English | 简体中文), fields for 'User Name' and 'Password', and buttons for 'Forget Password', 'Register', and 'Login'. A red circle highlights the 'Installer Tools' link at the bottom right.

After login, you will be prompt to create a new network. Enter a new network name.

Fig M1.6.2a –CloudManager Sign-in Prompt

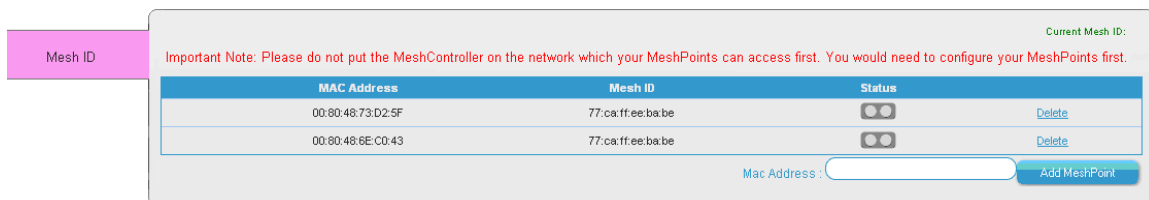
Step 3

Next, open the **Mesh ID** tab page from the menu.

Enter in the **MAC Address** box, the MP's Wireless Backhaul MAC Address.

Then click **Add MeshPoint** button to add to the list.

If there is more than one MP, repeat the step to enter each one into the table.



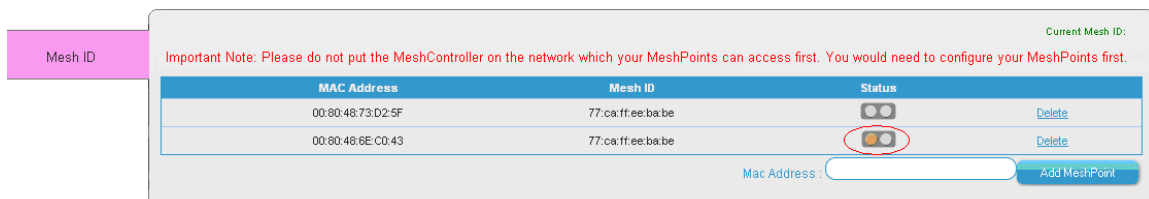
The screenshot shows the 'Mesh ID' tab interface. It includes a 'Current Mesh ID' label, an important note, a table with columns 'MAC Address', 'Mesh ID', and 'Status', and an 'Add MeshPoint' button. The table contains two entries with MAC addresses 00:80:48:73:D2:5F and 00:80:48:6E:C0:43, both with Mesh ID 77:ca:ffee:babe and Status indicators.

MAC Address	Mesh ID	Status
00:80:48:73:D2:5F	77:ca:ffee:babe	
00:80:48:6E:C0:43	77:ca:ffee:babe	

Fig M1.6.2b –Add MP in Mesh ID tab

Step 4

When an MP has checked-in to this new network in the CM, the four LEDs on that MP will light up. At the same time in the table, the **Status** display for that MP, the 1st indicator, will turn **orange** color. It will stay in **orange** color when all MPs have not checked-in. See **Fig M1.6.2c** below.



The screenshot shows the 'Mesh ID' tab interface, similar to Fig M1.6.2b, but the status indicator for the second MP (MAC 00:80:48:6E:C0:43) is highlighted with a red circle, indicating it is orange.

MAC Address	Mesh ID	Status
00:80:48:73:D2:5F	77:ca:ffee:babe	
00:80:48:6E:C0:43	77:ca:ffee:babe	

Fig M1.6.2c –Status when all MPs have not checked-in

Wait for 10 minutes, once all the MPs to have check-in the 1st status indicator turn **green** color, and the **Change Mesh ID** button will appear (see **Fig M1.6.2d**).

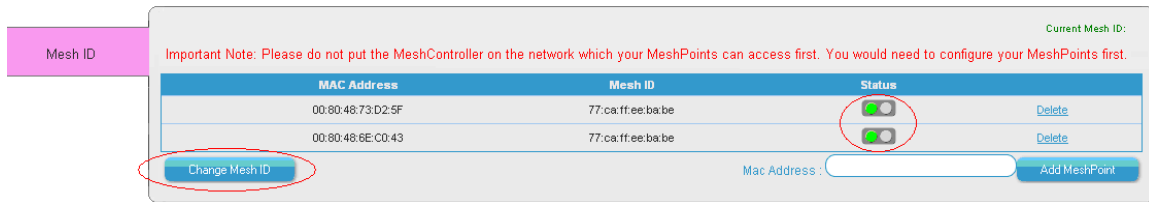


Fig M1.6.2d –Status after all MPs have checked-in

Step 5

Now click the **Change Mesh ID** button and enter a new Mesh ID.

You can create your own Mesh ID but it must be of the format, XX:XX:XX:XX:XX:XX where X is a hex number (0 -9 and a-f).

Assuming the current Mesh ID is 77:ca:ff:ee:ba:be and you want to change to the new Mesh ID, 78:ca:ff:ee:ba:be, then enter this new Mesh ID.

After an MP have updated to the new Mesh ID, the 2nd status indicator will turn **orange** color. See **Fig M1.6.2e** below. It will remains in **orange** color when all MPs have not updated the new Mesh ID.

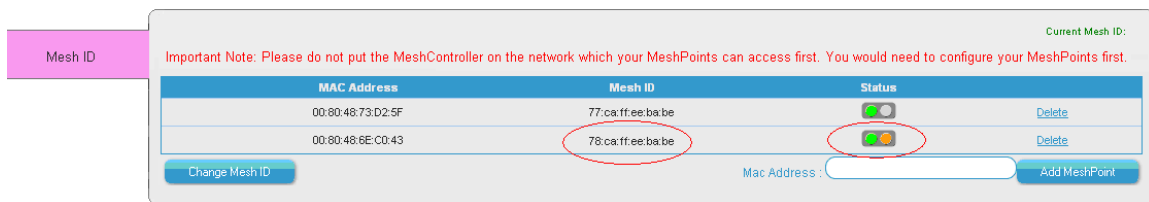
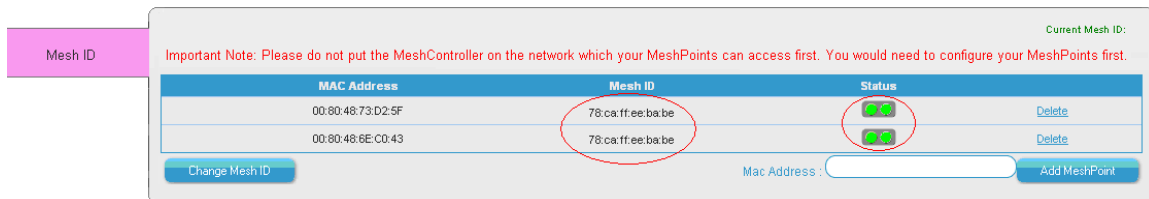


Fig M1.6.2e –Status when all MPs have not updated the Mesh ID

In about 10 minutes, once all the MPs have updated the new Mesh ID, the 2nd status indicator will changed from **orange** to **green** color. Now both 1st and 2nd status indicators will display **green** color and the new Mesh ID is displayed in the **Mesh ID** column in the table.

See **Fig 1.6.2f** below.

This indicates all the MPs have successfully updated the new Mesh ID.



FigM1.6.2f –Status after all MPs have updated the Mesh ID

Step 6

Install the MPs back in the R&D department. MPs with the new Mesh ID will form a separate and isolated wireless mesh network. While the Sales department will form another wireless mesh network next door. Thus, two virtual wireless mesh networks are created.

Process is now completed.

G1 Glossary Terms

Terms	Descriptions
Access Point (AP)	Generic term, 802.11 Infrastructure Access Point, no mesh capabilities
MeshPoint (MP)	Compex indoor, outdoor AP with mesh capabilities
Mesh node	Generic term, an AP on a mesh network
Mesh network	Generic term, Wireless mesh network built with AP connected in a mesh
MeshSpan	Compex long-distance mesh backhaul network, consisting of interconnected MeshPods
MeshPod	Individual long-distance wireless connecting devices to form a Compex MeshSpan
MeshSpan node	Consist of several MeshPods connected together through Ethernet
Mesh Gateway	A mesh node that connects its WAN port to WAN (or DHCP server). Mesh gateway breaks the mesh path down to shorter rote to shared resources.
Mesh Bridge	A MeshPoint that connects its LAN port to a LAN network.